



Docket No.: 62807-037

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#6

In re Application of

Shinji ITOH, et al.

Serial No.: 10/074,239

Group Art Unit: 2131

Filed: February 14, 2002

Examiner:

For: NETWORK SYSTEM ENABLING TRANSMISSION CONTROL

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Honorable Commissioner for Patents and Trademarks
Washington, D. C. 20231

Sir:

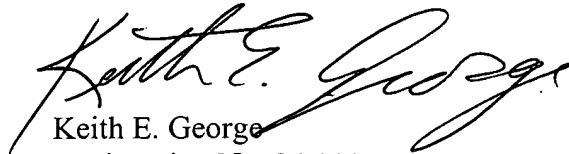
At the time the above application was filed, priority was claimed based on the following application:

Japanese Patent Application No. 2001-370824, filed December 5, 2001

A copy of each priority application listed above is enclosed.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202)756-8000 KEG:prp
Facsimile: (202)756-8087
Date: July 16, 2002



日 本 国 特 許 庁

JAPAN PATENT OFFICE

62807-037
Hoh et al.
Feb. 14, 2002
10/074,239
McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年12月 5日

出 願 番 号

Application Number:

特願2001-370824

[ST.10/C]:

[JP2001-370824]

出 願 人

Applicant(s):

株式会社日立製作所

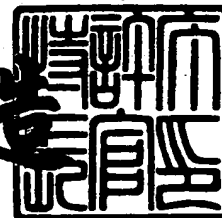
CERTIFIED COPY OF
PRIORITY DOCUMENT

Best Available Copy

2002年 2月22日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2002-3009442

【書類名】 特許願

【整理番号】 K01014091A

【あて先】 特許庁長官

【国際特許分類】 H04L 12/00

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 伊藤 信治

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 宮崎 邦彦

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 越前 功

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

【物件名】 要約書 1
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 送信制御可能なネットワークシステム

【特許請求の範囲】

【請求項 1】

組織内ネットワークに接続され、データを送受信する手段を備える送受信端末と、前記送受信端末と前記組織内ネットワークとの間で送受信されるデータを中継する手段を備える中継装置とを備えるネットワークシステムであって、

前記データは情報本体と前記情報本体に関連した付加情報からなり、

前記中継装置は前記付加情報を用いて送受信端末からのデータの送信を制御する手段と、前記組織内ネットワーク外へ送信可能な前記データから前記付加情報を取り除く手段を備える送信制御可能なネットワークシステム。

【請求項 2】

請求項 1 記載の送信制御可能なネットワークシステムであって、

前記付加情報は前記情報本体の属性を表す情報を有し、

前記中継装置は前記属性に応じた送信ポリシーを保持する手段と、

前記送信ポリシーに従って前記送受信端末が送信したデータの送信の可否を決定する手段とを備える

送信制御可能なネットワークシステム。

【請求項 3】

請求項 1 または請求項 2 記載の送信制御可能なネットワークシステムであって

前記属性は機密レベルである

送信制御可能なネットワークシステム。

【請求項 4】

請求項 3 記載の送信制御可能なネットワークシステムであって、

さらに、前記付加情報は前記機密レベルの設定者情報と、前記設定者の階級情報を有する、送信制御可能なネットワークシステム。

【請求項 5】

請求項 3 または請求項 4 に記載の送信制御可能なネットワークシステムであって、

前記送受信端末は前記付加情報を用いた前記情報本体へのアクセス制御手段と

前記データの内、情報本体を、当該送受信端末で動作するアプリケーションプログラムに渡す手段とを備える、送信制御可能なネットワークシステム。

【請求項 6】

請求項 4 に記載の送信制御可能なネットワークシステムであって、

さらに、前記付加情報を変更する手段を備える、送信制御可能なネットワークシステム。

【請求項 7】

請求項 5 または請求項 6 に記載の送信制御可能なネットワークシステムであって

前記アクセス制御手段は、前記アプリケーションプログラムに機密レベルを設定する手段と、前記アプリケーションプログラムのデータアクセス要求に対して、前記アプリケーションプログラムの機密レベルとデータ本体の機密レベルを比較することによって、前記アプリケーションプログラムの前記データへのアクセスの可否を決定する手段を備え、

前記アプリケーションプログラムに機密レベルを設定する手段は、の機密レベルは、当該アプリケーションプログラムが前記データの処理を開始する時に当該データ本体の機密レベルに応じて、前記アプリケーションプログラムに機密レベルを決定することを特徴とする、送信制御可能なネットワークシステム。

【請求項 8】

請求項 1 に記載の送信制御可能なネットワークシステムであって、前記中継装置は、

前記送受信端末が送信を許可されている、前記組織内ネットワーク外の送信先の送信許可リストと、

前記送受信端末が送信しようとするデータを暗号化する手段と、

前記送受信端末が送信しようとするデータを受信する手段と、前記送信許可リ

ストを参照して、前記データの送信の可否を決定する手段と、許可された場合に前記データを暗号化する手段と、前記暗号化データを、前記組織内ネットワーク外へ送信する手段を備える

送信制御可能なネットワークシステム。

【請求項 9】

請求項 1 記載の送信制御可能なネットワークシステムであって、前記中継装置は、

前記組織内ネットワーク外から前記送受信端末へ向けて送信されてきた情報本体を受信する手段と、

前記情報本体に付加情報を取りつけ、前記データを生成する手段と、

前記データを前記送受信端末に送信することを特徴とする、送信制御可能なネットワークシステム。

【請求項 10】

請求項 1 記載の送信制御可能なネットワークシステムであって、前記送受信端末は、

各情報本体に付加すべき付加情報を記録した付加情報リストと、前記付加情報をデータの送信時とリムーバブルメディアへの書き込み時に前記情報本体に付加し、データを生成する手段を備える

送信制御可能なネットワークシステム。

【請求項 11】

請求項 1 記載の送信制御可能なネットワークシステムであって、

前記付加情報は前記情報本体の機密レベルを表す情報と、前記情報本体の特徴値と、前記機密レベルを表す情報と前記特徴値に対する第 1 のデジタル署名と、前記機密レベルを表す情報と前記情報本体に対する第 2 のデジタル署名とから成る

送信制御可能なネットワークシステム。

【請求項 12】

請求項 1 記載の送信制御可能なネットワークシステムであって、

前記送受信端末は、第 1 の OS と第 2 の OS と前記第 1 の OS と第 2 の OS を

制御する複数OS制御プログラムとを備え、

前記第1のOSは前記情報本体を扱うアプリケーションプログラムを管理し、

前記第2のOSは前記付加情報を用いた前記情報本体へのアクセス制御手段と、前記付加情報を変更する手段とを管理する送信制御可能なネットワークシステム。

【請求項13】

第1の記憶装置とリムーバブルメディアを読み書きする第2の記憶装置と、前記第1、第2の記憶装置へのアクセス手段と、各情報本体に付加すべき付加情報のリストである付加情報リストを備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、前記第1の記憶装置内の情報本体を前記第2の記憶装置へ記録する記録手段を備え、

前記記録手段は、前記付加情報リストに記録されている前記情報本体の付加情報を参照して前記データの暗号化の可否を決定する手段と、暗号化可能な場合に暗号化鍵を生成する手段と、前記暗号化鍵を用いて前記データを暗号化する手段と、前記鍵管理装置に前記暗号化鍵を登録する手段と、前記鍵管理装置から登録した前記暗号化鍵の識別子を受信する手段と、前記情報本体に前記付加情報を付加しデータを生成する手段と、前記データを前記暗号化鍵を用いて暗号化したデータと前記識別番号を第2の記憶装置へ記録する手段とを備える、送信制御可能なネットワークシステム。

【請求項14】

第1の記憶装置とリムーバブルメディア対応の第2の記憶装置と、前記第1、第2の記憶装置へのアクセス手段と各情報本体に付加すべき付加情報のリストである付加情報リストを備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、第2の記憶装置内のデータを第1の記憶装置へ記録する記録手段を備え、

前記データは識別子と暗号化データを有し、

前記暗号化データは付加情報部を有し、

前記記録手段は、前記識別子を前記鍵管理装置に送信し、対応する前記暗号化データの暗号化鍵を受信する手段と、

前記暗号化データを前記暗号化鍵を用いて復号化する手段と、前記付加情報を前記付加情報リストに追加する手段とを備え、

前記鍵管理装置は、前記記録手段から前記識別子を受信し、対応する前記暗号化データの暗号化鍵を前記記録手段に送信する手段を備える送信制御可能なネットワークシステム。

【請求項 1 5】

第1の記憶装置とリムーバブルメディアを読み書きする第2の記憶装置と、前記第1、第2の記憶装置へのアクセス手段を備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、前記第1の記憶装置内のデータを前記第2の記憶装置へ記録する記録手段を備え、

前記データは情報本体と前記情報本体に関連した付加情報とからなり、

前記記録手段は前記付加情報に基づき前記データの暗号化の可否を決定する手段と、暗号化鍵を生成する手段と、前記暗号化鍵を用いて前記データを暗号化する手段と、前記鍵管理装置に前記暗号化鍵を登録する手段と、前記鍵管理装置から登録した前記暗号化鍵の識別子を受信する手段と、前記暗号化したデータと前記識別子とを第2の記憶装置へ記録する手段と、を備え、

前記鍵管理装置は、前記記録手段から前記暗号化鍵を受信し、対応する前記識別子を前記記録手段に送信する手段を備える送信制御可能なネットワークシステム。

【請求項 1 6】

第1の記憶装置とリムーバブルメディアを読み書きする第2の記憶装置と、前記第1、第2の記憶装置へのアクセス手段を備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、前記第2の記憶装置内のデータを前記第1の記憶装置へ記録する記録手段を備え、

前記データは識別子と暗号化データを有し、

前記記録手段は前記識別子を前記鍵管理装置に送信し、前記暗号化データの暗号化鍵を受信する手段と、前記暗号化データを前記暗号化鍵を用いて復号化する手段を備え、

前記鍵管理装置は、前記記録手段から前記識別子を受信し、対応する前記暗号化データの暗号化鍵を前記記録手段に送信する手段を備える
送信制御可能なネットワークシステム。

【請求項 17】

請求項 4 記載の送信制御可能なネットワークシステムであって、

前記送受信端末は、前記付加情報の変更手段を有し、

前記変更手段は、前記付加情報のデータの機密レベルと前記機密レベルの設定者情報と前記設定者の階級情報と、前記データの付加情報を変更しようとする者の変更者情報と前記変更者の階級情報とを参照し、前記データの機密レベルの変更の可否を決定する

送信制御可能なネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は組織などで扱う機密情報が外部に漏洩することを防止するための技術に関する。

【0002】

【従来の技術】

企業などで扱う電子データには多くの社外秘情報が含まれる。これらの電子データには、意図的に文書内に「社外秘」と書き込むことによって閲覧者にその電子データが社外秘であることを伝える。外部に漏らさないように意識させることによって、社外秘データが外部に漏れることを防止している。しかしながら、ときには社外秘データを不注意または意図的にメールで外部に送信してしまう可能性がある。これらの問題に対して、サーバ側でメールの内容をキーワード検索することにより、社外秘情報と思われるあらかじめ設定したキーワード（例：社外秘）が含まれていないかどうかのチェックを行うことにより、そのキーワードが

含まれていない場合には、そのまま送信を行い、含まれている場合には送信を停止する。

【 0 0 0 3 】

また、企業内においても幹部しか参照することができない機密情報といったものが存在する。この機密情報が権限のない社員に参照されないように、強制アクセス制御機能を付加することにより、そのような機密情報が一般社員に参照されないように情報フロー制御を行うことが可能である。

【 0 0 0 4 】

強制アクセス制御については、文献 [TCSEC] : 「Department of Defense Trusted Computer System Evaluation Criteria」アメリカ国防総省標準 (DOD 5200.28-STD) に詳しい。

また、従来、ネットワーク環境におけるマルチレベルセキュリティを実現するための技術として、米国特許5,940,591がある。

また、データを暗号化して送信することにより、機密情報の第3者への漏洩を防止する方法が、特開平8-204701号公報に開示されている。

【 0 0 0 5 】

【発明が解決しようとする課題】

キーワード検索に基づく情報漏洩を防止するシステムの場合、特定のデータフォーマットに対して有効であるが、未対応のデータフォーマットや文書情報が含まれない画像ファイルなどに対しては有効ではない。

【 0 0 0 6 】

また、強制アクセス制御機能を備える計算機の場合、その計算機内では十分な情報フロー制御を行うことは可能であるが、別の計算機にデータが移動した場合には、移動先の計算機のシステムに依存する為、データの機密レベルを保証することが困難となる。また、強制アクセス制御機能を備える計算機は特殊用途向けに利用されることが多く、汎用のアプリケーションを利用できないため、一般の企業や組織には普及しづらい。

【 0 0 0 7 】

また、上記米国特許5,940,591号では、(1) ユーザ単位のアクセス制御は提

供されているもののファイル単位のアクセス制御は行えない、(2) 送信のたびにSMへの問い合わせが必要になり負荷が高い、などの課題がある。

【0008】

また、データを暗号化して送信する場合、データを暗号化するのは社員の端末側であり、社員がどのデータが社外秘情報であるということを知っている必要がある。その為、不注意に社外秘データを暗号化せずに送信してしまう恐れがある。

【0009】

【課題を解決するための手段】

本発明は、データの送信者の不注意により組織内の機密情報が外部へ送信されるのを防止する技術を提供する。

本発明は、上記技術を任意のデータフォーマットに対して適用可能なシステムを提供する。

本発明は、また、組織内でのデータの移動においてもデータの機密レベル（機密、非機密）を維持するとともに、それを任意のデータフォーマットに対して適用可能な技術を提供する。

【0010】

具体的には、情報本体(データ本体)に、情報本体の属性を表す付加情報を付加し、付加情報を用いて、情報本体の送受信を制御する。

より具体的には、各データ本体(情報本体)に、属性を表すラベル（付加情報）をデータ本体に付加し、組織内ではラベル付きのデータを扱うようにする。属性としては、例えば機密レベル（社外秘、一般など）がある。外部へデータを送信する場合には、ゲートウェイサーバ上の送信管理プログラムがこのラベルをチェックし、外部へ送信してよいかどうかを決定し、外部へ送信可能であれば、データに付加されているラベルを取り除いて、データ本体を外部へ送信する。また、ゲートウェイサーバは外部からデータ本体を受信した場合には、データ本体にラベルを取り付け、組織内のデータの送信先にデータを送信する。

【0011】

また、ユーザが利用する端末においては、データ本体に直接ラベルを付加する

のではなく、各データの機密レベル情報を別のファイルに書き込んでも良い。クライアント端末からデータ本体を送信する時に上記ファイルを参照し、データ本体の機密レベルを表すラベルを付加し、ラベル付きのデータを送信すればよい。

また、ラベルに署名をつけることによって、ラベルを不正に改ざんされる恐れを防止することができ、さらに、誰が機密レベルを設定したかを保証することが可能となる。

【0012】

また、本発明は、アプリケーションプログラムとデバイスドライバのバグ、さらにはユーザの操作ミスによるラベルの不正な変更や破壊を防止する技術を提供する。具体的には複数OS制御技術を用いて、2つのOSを動作させ、一方のOSをユーザが利用可能とし、もう一方のOSはラベル管理専用として用いる。

【0013】

本発明によれば、上記米国特許と比較して、(1) アクセス制御リストによりデータ単位のアクセス制御が可能である、(2) アクセス制御リストは各ユーザ端末内にあるため毎回の問い合わせは不要、といった特徴を備える。

【0014】

【発明の実施形態】

(第1の実施例)

本発明の第1の実施形態を説明する。本実施例では、ファイルに格納されたデータの先頭には機密レベルを表すラベルが付いており、このラベル情報を利用して、情報フロー制御を行う。機密レベルの内容やレベル数は、システムごとに自由に設定できるが、以下では「社外秘」「一般」の2段階の場合について説明する。なお、このラベルはファイルによって、ラベルを付けたら付かなかったりしても良い。例えば、システムファイル、ドライバファイルにはラベルを付けずに、アプリケーションのデータファイルにラベルを付ける。ラベルが付いていないファイルの取り扱い、システムのポリシーとしてあらかじめ決めておく。本実施例において、ラベルが付いていないファイルは、クライアント端末側では「一般」のデータとして扱うものとする。

【0015】

図1は本実施例のシステムの構成例である。1つ以上のクライアント端末101とゲートウェイサーバ118と鍵管理サーバ114が組織内ネットワーク117に繋がっており、さらに、ゲートウェイサーバ118は組織外ネットワーク121に繋がっている。クライアント端末101には、CPU113、メモリ102、磁気ディスク106、ネットワークI/F112、外部記憶装置122がある。メモリ102上には、ラベル管理プログラム109、ファイルシステムドライバ104、ディスクドライバ105、プロトコルドライバ110、ネットワークアダプタドライバ111、アプリケーションプログラム103、機密レベル変更プログラム108がロードされている。上記各プログラムは、OS(Operating System)の管理のもとで動作する。

【0016】

磁気ディスク106内には複数のファイル107が格納されている。外部記憶装置122は、取り外し可能な記憶媒体（以下、リムーバブルメディアという）123内のファイル124からデータを読み取ったり、書き込んだりする装置である。外部記憶装置としては、例えば、フロッピーディスクドライブやCD-ROM装置などがある。ゲートウェイサーバ118には、送信管理プログラム119と受信管理プログラム120が動作している。鍵管理サーバ114には、鍵情報116があり、さらに鍵管理プログラム115が動作している。クライアント端末101はラベル付きファイルをネットワーク上に送信し、ゲートウェイサーバ118は当該ラベル付きファイルのラベルのチェックを行い、外部に当該ラベル付きファイルを送信してよいかどうかを決定する。

【0017】

各実施例における各プログラムは、磁気ディスク106や、リムーバブルメディアや、組織内、組織外ネットワークに接続された他のサーバから、メモリ102に導入されても良い。

【0018】

図2は、本実施例におけるラベルのフォーマットを例示している。ラベルはファイル107の先頭にあり、32ビット（4バイト）の情報をもつ。32ビットうちの最初の2ビットがラベルのフォーマットのバージョン情報201を表し、

次の3ビットがファイル107の機密レベル202を表し、次の3ビットがファイル107の機密レベルを設定した設定者レベル203を表し、残りの24ビットがファイル107の機密レベルを設定した設定者ID204を表す。機密レベル202は、「一般」「社外秘」などであり、設定者レベル203は、例えば「社員」「係長」「課長」「部長」などである。なお、ラベルは機密レベル202の数や組織の規模、さらにその他の情報を付加したい場合など、組織によって異なるフォーマット、サイズにしても良い。その他の情報としては、例えば、ラベルの有効期限やファイル107の作成者情報、アクセス制御情報（読み取り専用など）がある。機密レベル202を用いるのではなく、その他の様々な情報を用いたアクセス制御を行ってもよい。

【0019】

ラベル管理プログラム109は、ファイル107のラベルの管理を行い、アプリケーションプログラム103がファイル107にアクセスする場合にはラベルを取り外し、ラベル以外のデータ（データ本体）をアプリケーションプログラム103に渡す。また、アプリケーションプログラム103がファイル107をネットワークI/F112を介して組織内ネットワーク117上に送信する場合には、ラベル管理プログラム109はラベルが付いた状態で送信を行う。

【0020】

図3は、本実施例における磁気ディスク106上にあるファイル107のオープンの処理フロー図である。ファイルのオープンとは、ファイル内のデータの読み取り、またはファイル内へのデータの書き込みなどの操作を可能にするための前処理である。

ステップ301では、アプリケーションプログラム103がファイル107のオープン要求をOSのI/Oマネージャを通じてラベル管理プログラム109に出す。

ステップ302では、ラベル管理プログラム109はアプリケーションプログラム103のプロセスIDをI/Oマネージャを通じて取得する。プロセスとは、OSが管理するプログラムの実行単位であり、プロセスIDはプロセスの識別子である。

【 0 0 2 1 】

ステップ 3 0 3 では、ラベル管理プログラム 1 0 9 は当該ファイル 1 0 7 の機密レベル 2 0 2 をチェックする。当該ファイル 1 0 7 にラベルが付いていない場合には、当該ファイル 1 0 7 は「一般」とであると判断する。ラベルが付いていない例としては、システムファイル、ドライバファイルなどがある。

ステップ 3 0 4 では、ラベル管理プログラム 1 0 9 はプロセス ID からアプリケーションプログラム 1 0 3 の機密レベルをチェックする。ラベル管理プログラム 1 0 9 は、図 4 に示すプロセス管理リスト 4 0 0 を参照することにより、アプリケーションプログラム 1 0 3 の機密レベルを調べる。アプリケーションプログラム 1 0 3 がファイル 1 0 7 をオープンしていない時点でのアプリケーションプログラム 1 0 3 の機密レベルは未設定となっている。

【 0 0 2 2 】

アプリケーションプログラムの機密レベル（実行中のプロセスの機密レベル）の必要性は次の通り。アプリケーションプログラム 1 0 3 そのものは、様々な機密レベルのファイルを扱うことができる。機密ファイルと非機密ファイルを同時に扱っている場合、機密情報が非機密ファイルの中に書き込まれてしまうことがあり得る（例えば、カット＆ペーストなど）。本実施例においては、プロセスの機密レベルを利用することにより、このような危険を防止する。

【 0 0 2 3 】

図 4 はプロセス管理リスト 4 0 0 を表している。1 列目にプロセス ID 4 0 1、2 列目に当該プロセス機密レベル 4 0 2（アプリケーションプログラムの機密レベル）、3 列目にオープンしているファイル名 4 0 3、4 列目に当該ファイル 1 0 7 の機密レベル 4 0 4 が示されている。プロセス管理リスト 4 0 0 は、ラベル管理プログラム 1 0 9 のロード時にラベル管理プログラム 1 0 9 が作成し、初期化を行う。また、ラベル管理リスト 4 0 0 の更新もラベル管理プログラム 1 0 9 が行う。

【 0 0 2 4 】

続いて、ステップ 3 0 5 では、ラベル管理プログラム 1 0 9 はアプリケーションプログラム 1 0 3 の機密レベル 4 0 2 が設定済みであるかどうかチェックし、

設定済みである場合にはステップ311へ進み、未設定の場合にはステップ306へ進む。

ステップ306では、ラベル管理プログラム109はアプリケーションプログラム103のプロセスIDをプロセス管理リスト400に追加する。

ステップ307では、ラベル管理プログラム109はアプリケーションプログラム103のプロセス機密レベル402を当該ファイル107の機密レベル202に設定する。

ステップ308では、ラベル管理プログラム109はプロセス管理リスト400に当該ファイル107のファイル名403と機密レベル202を追加する。

ステップ309では、ラベル管理プログラム109は当該ファイル107のオープン要求をファイルシステムドライバ104に送信する。

ステップ310でファイルオープン成功となる。

【0025】

ステップ311では、ラベル管理プログラム109はアプリケーションプログラム103の機密レベル402が当該ファイル107の機密レベル202と一致しているかどうかをチェックする。一致している場合にはステップ308へ進み、一致していない場合にはステップ312へ進む。

ステップ312では、ラベル管理プログラム109は当該ファイル107を本当にオープンするかどうかを利用者に選択させる為のメッセージを表示する。

ステップ313では、利用者がファイル107をオープンするかどうかの選択を行い、利用者がファイル107をオープンする、を選択した場合にはステップ314へ進み、利用者がファイル107をオープンしない、を選択した場合にはステップ315へ進む。

【0026】

ステップ314では、ラベル管理プログラム109はアプリケーションプログラム103の機密レベル402が当該ファイル107の機密レベル202より高いかどうかのチェックを行い、アプリケーションプログラムの機密レベル402の方が高い場合にはステップ308へ進み、低い場合にはステップ307へ進む。

ステップ 3 1 5 では、ラベル管理プログラム 1 0 9 は当該ファイル 1 0 7 のオープンエラーメッセージをアプリケーションプログラム 1 0 3 に送信する。

ステップ 3 1 6 でファイルオープン失敗となる。

【 0 0 2 7 】

本実施例は、ユーザの指定次第でアプリケーションプログラム 1 0 3 が必ずファイル 1 0 7 をオープンすることが可能なように構成しているが、図 3 のステップ 3 1 1 において、アプリケーションプログラム 1 0 3 の機密レベル 4 0 2 がファイル 1 0 7 の機密レベル 2 0 2 と一致していない場合には、ステップ 3 1 5 に進み、ファイルオープン要求を強制的に拒否するように構成しても良い。

【 0 0 2 8 】

また、ファイルの新規作成時には、当該ファイルの機密レベル 2 0 2 を利用者が選択する形式をとる。標準設定では、アプリケーションプログラム 1 0 3 の機密レベル 4 0 2 と等しくなるようにし、アプリケーションプログラム 1 0 3 の機密レベル 4 0 2 が「未設定」の場合には、最上位の「社外秘」が選ばれるようにすることが望ましい。

【 0 0 2 9 】

図 5 は、本実施例におけるファイル 1 0 7 からデータを読み取る場合の処理フロー図である。ここでは例としてアプリケーションプログラム 1 0 3 がファイル 1 0 7 の先頭からのアドレスであるバイトオフセット 0xAB00 を読み取る場合について記述する。0x は 16 進数を示す。

ステップ 5 0 1 では、アプリケーションプログラム 1 0 3 がファイル 1 0 7 のバイトオフセット 0xAB00 からデータを読み取る要求を出す。

ステップ 5 0 2 では、ラベル管理プログラム 1 0 9 がバイトオフセット 0xAB00 を実際のバイトオフセット 0xAB04 に変換する。本実施例のファイル 1 0 7 はファイル 1 0 7 の先頭に 4 バイト（32 ビット）の情報（ラベル）が付いているが、アプリケーションプログラム 1 0 3 はラベルがあることを知らないため、アプリケーションプログラム 1 0 3 が読み取りを要求するバイトオフセットを調整する必要がある。そのため、本実施例ではアプリケーションプログラム 1 0 3 が要求するバイトオフセットにラベル情報のバイト長である 4 バイトを追加した値が実

際のバイトオフセットとなる。

ステップ 5 0 3 では、ファイルシステムドライバ 1 0 4 は実際のバイトオフセット 0xAB04 を磁気ディスク 1 0 6 上の相対位置に変換する。

ステップ 5 0 4 では、ディスクドライバ 1 0 5 は磁気ディスク 1 0 6 の相対位置を物理的な位置に変換してデータをメモリ 1 0 2 に読み込む。

【 0 0 3 0 】

図 6 は、本実施例におけるファイル 1 0 7 ヘータを書き込む場合の処理フロー図である。ここでは例としてアプリケーションプログラム 1 0 3 がファイルの特定のバイトオフセット 0xAB00 に書き込む場合について記述する。

ステップ 6 0 1 では、アプリケーションプログラム 1 0 3 がファイル 1 0 7 のバイトオフセット 0xAB00 にデータを書き込む要求を出す。

ステップ 6 0 2 では、ラベル管理プログラム 1 0 9 はアプリケーションプログラム 1 0 3 の機密レベル 4 0 2 と当該ファイル 1 0 7 の機密レベル 2 0 2 をチェックする。

ステップ 6 0 3 では、ラベル管理プログラム 1 0 9 はアプリケーションプログラム 1 0 3 と当該ファイル 1 0 7 の機密レベルが一致しているかどうかをチェックし、一致している場合にはステップ 6 0 5 へ進み、一致していない場合にはステップ 6 0 4 へ進む。

【 0 0 3 1 】

ステップ 6 0 5 では、ラベル管理プログラム 1 0 9 がバイトオフセット 0xAB00 を実際のバイトオフセット 0xAB04 に変換する。上述したアプリケーションプログラム 1 0 3 がファイル 1 0 7 のデータを読み込む場合と同様、アプリケーションプログラム 1 0 3 が要求するバイトオフセットに 4 バイト追加した値が実際のバイトオフセットとなる。

ステップ 6 0 6 では、ファイルシステムドライバ 1 0 4 は実際のバイトオフセット 0xAB04 を磁気ディスク 1 0 6 上の相対位置に変換する。

ステップ 6 0 7 では、ディスクドライバ 1 0 5 は磁気ディスク 1 0 6 の相対位置を物理的な位置に変換してデータを磁気ディスク 1 0 6 に転送する。

【 0 0 3 2 】

ステップ604では、ラベル管理プログラム109は当該ファイル107の機密レベル202をアプリケーションプログラム103の機密レベル402に変更し、さらに、設定者レベル203、設定者ID204についても変更し、ステップ605へ進む。本実施例では、ステップ604で強制的にアプリケーションプログラム103の機密レベル402にファイル107の機密レベル202を変更したが、利用者がファイル107の機密レベル202を選択できるようにメッセージを表示しても良い。

【0033】

本実施例のクライアント端末101には、外部記憶装置122があり、リムーバブルメディア123を用いてデータを別の端末に移動することができる。そのため、リムーバブルメディアを介して外部へ情報が漏洩するおそれがあるため、リムーバブルメディア123内のデータを外部の不正アクセスから保護する必要がある。

【0034】

図7は、本実施例におけるリムーバブルメディア123へのファイル107の書き込みの処理フロー図である。ここでは、アプリケーションプログラム103が新規にファイル124を作成し、作成したファイル124にファイル107のデータをコピーする場合を説明する。ファイル124の機密レベルは、アプリケーションプログラム103が、ファイル124にデータを書き込む際に設定する。

【0035】

ステップ701では、アプリケーションプログラム103がリムーバブルメディア123内のファイル124にファイル107のデータを書き込む要求を出す。

ステップ702では、ラベル管理プログラム109はファイル107の機密レベル202をチェックする。

ステップ703では、当該ファイル107の機密レベル202が「社外秘」であるかどうかを確認し、機密レベル202が「一般」の場合にはステップ704へ進み、「社外秘」の場合にはステップ706へ進む。

【0036】

機密レベル202が「一般」の場合、ステップ704において、ラベル管理プログラム109はリムーバブルメディア123内のファイル124へ当該ファイル107のラベル以外のデータを書き込む要求を出す。

ステップ705では、ファイルシステムドライバ104が書き込み要求を受け取り、ディスクドライバ105がリムーバブルメディア123へ当該ファイル107のデータを転送する。

【0037】

機密レベル202が「社外秘」の場合、ステップ706においては、ラベル管理プログラム109は暗号化鍵と復号化鍵を生成する。暗号化鍵と復号化鍵は同一であっても良い。

ステップ707では、ラベル管理プログラム109は復号化鍵を鍵管理サーバ114に登録し、識別子(例えば、ID番号)を鍵管理サーバ114から受け取る。

ステップ708では、ラベル管理プログラム109は当該ファイル107を、暗号化鍵を用いて暗号化し、暗号化ファイルを作成する。暗号化ファイルはID番号と暗号化データとから成る。ID番号はラベル管理プログラム109が暗号化ファイルの作成時に付加する。

ステップ709では、ラベル管理プログラム109はリムーバブルメディア123内のファイル124へ暗号化ファイルのデータを書き込む要求を出し、ステップ705へ進む。

【0038】

また、既存のファイル124のデータを更新する場合で、データが暗号化されている場合には、ラベル管理プログラム109は、ファイル124に含まれているID番号を鍵管理サーバ114に送信し、鍵管理サーバ114から暗号化鍵を受信する。ラベル管理プログラム109は受信した暗号化鍵を用いてデータを暗号化し、ファイル124に暗号化データを書き込む。

【0039】

図8はリムーバブルメディア123内のファイル124からデータを読み取る場合の処理フロー図である。

ステップ801では、アプリケーションプログラム103が、ラベル管理プログラム109に対して、リムーバブルメディア123内のファイル124からデータを読み取る要求を出す。

ステップ802では、ラベル管理プログラム109は、ファイルシステムドライバ104に対して、リムーバブルメディア123内の当該ファイル124からデータを読み取る要求を出す。

ステップ803では、ファイルシステムドライバ104が読み取り要求を受け取り、ディスクドライバ105がリムーバブルメディア123内の当該ファイル124からデータを読み込む。

ステップ804では、ラベル管理プログラム109は、読み出されたデータを受け取り、当該データが暗号化されているかをチェックする。

ステップ805では、当該データが暗号化されていない場合にはステップ806へ進み、暗号化されている場合にはステップ807へ進む。

【0040】

ステップ806では、ラベル管理プログラム109はアプリケーションプログラム103にデータを渡す。

ステップ807では、ラベル管理プログラム109は当該ファイル124のID番号を読み取る。

ステップ808では、ラベル管理プログラム109は当該ファイル124のID番号を鍵管理サーバ114に送信し、当該ファイル124の復号化鍵を受け取る。

ステップ809では、ラベル管理プログラム109は暗号化されているデータを、復号化鍵を用いて復号化し、ステップ806へと進む。

ステップ808でのクライアント端末101と鍵管理サーバ114間の通信はデータを暗号化しても良い。

【0041】

リムーバブルメディア123上のファイル124のデータを磁気ディスク106のファイル107へコピーまたは移動する場合で、当該ファイル124にラベルが付いていない場合は、ラベル管理プログラム109は当該ファイル124に

「一般」のラベルを付けて、磁気ディスク106に保存する。

【0042】

図9はアプリケーションプログラム103がファイルをネットワーク117上へ送信する際の処理フロー図である。

ステップ901では、アプリケーションプログラム103がファイルを伴った当該ファイルの送信要求を出す。

ステップ902では、ラベル管理プログラム109は当該ファイル107の機密レベル202を取得し、ラベル付きファイルの送信要求に変換する。アプリケーションプログラム103は、送信対象データとして、ラベル無しのファイルデータを出力する為、ラベル管理プログラム109がラベル付きファイルに変換する。

ステップ903では、プロトコルドライバ110がラベル付きファイルをパケットに分割し、パケットヘッダを作成する。

ステップ904では、ネットワークアダプタドライバ111はLANコントローラを経由して外部へ当該ファイル107を送信する。

【0043】

次に、機密レベル変更プログラム108について説明する。機密レベル変更プログラム108は、ファイル107の機密レベル202を変更するためのプログラムである。図10は「社外秘」であるファイル107を「一般」に変更する場合の処理フロー図である。

ステップ1001では、機密レベル変更プログラム108がファイル107の機密レベル202を「社外秘」から「一般」に変更する要求を出す。

ステップ1002では、ラベル管理プログラム109はファイル107のラベルを読み込み、設定者ID204を取得する。

ステップ1003では、ステップ1002で取得した設定者ID204と機密レベル202の変更者IDが一致しているかどうかを判定する。一致している場合には、ステップ1004へ進み、一致していなければステップ1005へ進む。

【0044】

ステップ1004では、ラベル管理プログラム109は当該ファイル107の

機密レベル 2 0 2 を「一般」に変更し、設定者 ID 2 0 4、設定者レベル 2 0 3 も同時に変更する。

ステップ 1 0 0 5 では、機密レベル 2 0 2 の変更者が機密レベル 2 0 2 を変更できる権限を持っているかどうかを判定する。権限を持っていればステップ 1 0 0 4 へ進み、持っていなければステップ 1 0 0 6 へ進む。

ステップ 1 0 0 6 では、ラベル管理プログラム 1 0 9 はエラーメッセージを機密レベル変更プログラム 1 0 8 に渡す。

【 0 0 4 5 】

ステップ 1 0 0 5 において、機密レベル 2 0 2 を変更できる権限とは、強制的に機密レベル 2 0 2 を変更できる権限のことである。この権限は、機密レベル 2 0 2 を変更しようとする者のレベルがファイル 1 0 7 の設定者レベル 2 0 3 よりも高い場合に変更可能であるように設定することも可能である。また、機密レベル 2 0 2 を変更できるレベルを与えられていても、すべてのファイル 1 0 7 の機密レベル 2 0 2 を無条件に変更することは許さず、設定者 ID 2 0 4 によって変更できる場合と変更できない場合を設定することも可能である。また機密レベル 2 0 2 を変更できる権限のポリシーを組織毎に分けて設定しても良い。ここでは、機密レベル 2 0 2 を「社外秘」から「一般」に変更する場合について記述したが、機密レベル 2 0 2 が 3 以上の場合においても同様の手法により機密レベル 2 0 2 を下げることが可能である。

【 0 0 4 6 】

機密レベル変更プログラム 1 0 8 は、また、「一般」ファイル 1 0 7 を「社外秘」ファイル 1 0 7 に機密レベル 2 0 2 を上げる操作を行うことが可能である。機密レベル 2 0 2 を上げることによって、情報が漏れることはないという考えに従えば、機密レベル 2 0 2 を上げる操作は誰でも無条件に行うことが可能であるように設定しても良い。

【 0 0 4 7 】

送信管理プログラム 1 1 9 は、クライアント端末 1 0 1 が組織外ネットワーク 1 2 1 に送信しようとするファイル 1 0 7 のラベルをチェックし、当該ファイル 1 0 7 を送信してよいかどうかを決定する。図 1 1 はラベルのチェックの処理フ

ロー図である。

ステップ 1 2 0 1 では、ゲートウェイサーバ 1 1 8 は組織内のクライアント端末 1 0 1 から組織外ネットワーク 1 2 1 へ送信しようとするファイル 1 0 7 を受信する。

ステップ 1 2 0 2 では、送信管理プログラム 1 1 9 は当該ファイル 1 0 7 のラベルが付いているかどうかを判定する。

ステップ 1 2 0 3 では、ラベルが付いていればステップ 1 2 0 4 へ進み、付いていなければステップ 1 2 0 9 へ進む。

【 0 0 4 8 】

ステップ 1 2 0 4 では、送信管理プログラム 1 1 9 は当該ファイル 1 0 7 の機密レベル 2 0 2 をチェックする。

ステップ 1 2 0 5 では、当該ファイル 1 0 7 の機密レベル 2 0 2 が「一般」であればステップ 1 2 0 6 へ進み、「一般」でなければステップ 1 2 1 1 へ進む。

ステップ 1 2 0 6 では、送信管理プログラム 1 1 9 は当該ファイル 1 0 7 のラベルを取り外す。

ステップ 1 2 0 7 では、送信管理プログラム 1 1 9 は当該ファイル 1 0 7 を外部に送信する。

ステップ 1 2 0 8 でファイル送信成功となる。

【 0 0 4 9 】

ステップ 1 2 0 9 では、送信管理プログラム 1 1 9 は当該ファイル 1 0 7 が不正データであると判断し、エラーメッセージを送信元端末と、システム管理者が使用する装置に送る。

ステップ 1 2 1 0 でファイル送信失敗となる。

ステップ 1 2 1 1 では、送信管理プログラム 1 1 9 は当該ファイル 1 0 7 の機密レベル 2 0 2 が「社外秘」とあるというメッセージを送信元端末に送る。

ステップ 1 2 1 2 でファイル送信失敗となる。

【 0 0 5 0 】

ステップ 1 2 0 6 において、ラベルを取り外す理由は、ラベルが解釈できるのは本実施例のシステムが導入されている他のシステムや端末に限られるからとい

うポリシーに従うためである。したがって、本実施例においては、外部ヘファイルを送信する場合にはラベルを取り外すようにしているが、他のポリシーに従えば、これに限定されるものではない。

【 0 0 5 1 】

また、本実施例では、組織外に送信されるデータについては、ゲートウェイサーバ 1 1 8 上で組織外ネットワーク 1 2 1 に送信してよいかどうか判定された後、ラベルの取り外しをおこなわれるため、組織外ネットワーク 1 2 1 においても、透過的に利用可能である。

【 0 0 5 2 】

また、ゲートウェイサーバ 1 1 8 上に送信先許可リストを設けることにより、この送信先許可リストに記載された送信先ヘファイル 1 0 7 を送信する場合には、機密レベル 2 0 2 が「社外秘」の場合でも外部にファイル 1 0 7 を送信しても良い。この場合、送信管理プログラム 1 1 9 はファイル 1 0 7 を暗号化し、ラベルを取り外さずに送信する。さらに、送信管理プログラム 1 1 9 は送信元、送信先、送信ファイルをログに記録しておく。暗号鍵は、リムーバブルメディアへのファイル 1 0 7 の書き込みの場合と同様に鍵管理サーバ 1 1 4 に登録する。この場合の送信するファイル 1 0 7 は ID 番号と暗号化データを持つ。

【 0 0 5 3 】

次に、ゲートウェイサーバ 1 1 8 が組織外ネットワーク 1 2 1 からファイル 1 0 7 を受信した場合の処理について説明する。

まず、ゲートウェイサーバ 1 1 8 は組織外ネットワーク 1 2 1 からクライアント端末 1 0 1 へ向けて送信してきたファイル 1 0 7 を受信する。

次に、受信管理プログラム 1 2 0 は当該ファイル 1 0 7 に「一般」のラベルを取りつける。また、設定者 ID 2 0 4 はゲートウェイサーバ 1 1 8 の ID とし、設定者レベル 2 0 3 は最低レベルに設定する。

その後、受信管理プログラム 1 2 0 はクライアント端末 1 0 1 へ当該ファイル 1 0 7 を送信する。

【 0 0 5 4 】

また、受信管理プログラム 1 2 0 はラベル付きのファイル 1 0 7 を受信する機

能を備えていても良い。この場合、受信管理プログラム 1 2 0 はラベルが付いていることを確認したあと、当該ファイル 1 0 7 をクライアント端末 1 0 1 に送信する。

【 0 0 5 5 】

組織内ネットワーク 1 1 7 内の端末間（クライアント端末 1 0 1 間、クライアント端末 1 0 1 とゲートウェイサーバ 1 1 8 間など）は互いに認証を行ってもよい。端末（1 0 1、1 1 8、1 1 4）間の認証は、各端末がそれぞれ通信を許可している端末の MAC(Media Access Control)アドレス（または IP アドレス）のリスト（通信許可リスト）を持ち、各端末はこの通信許可リストを参照して認証を行う。各端末は、互いの通信許可リストに通信相手の MAC アドレス（または IP アドレス）があった場合に限り、端末間の通信が可能となるように制御すればよい。また、端末間の認証を各端末が行うのではなく認証サーバを設けることにより、この認証サーバが端末間の通信の許可を決定してもよい。この場合、各端末は認証サーバを経由して別の端末と通信を行う。また、端末間の認証は、公開鍵暗号方式を用いても良い。

【 0 0 5 6 】

さらに、認証サーバは、クライアント端末 1 0 1 が組織内または組織外の相手と送受信する全ファイルについて、そのラベルのチェックを行ってもよい。企業内においては社員の役職、または部署によってアクセス可能なファイル 1 0 7 とそうでないファイル 1 0 7 が存在するが、このような場合においても認証サーバがラベルのチェックを行うことにより、情報フロー制御を行うことが可能である。

【 0 0 5 7 】

（第 2 の実施例）

本発明の第 2 の実施形態を説明する。第 1 の実施例では、ファイル 1 0 7 の機密レベル 2 0 2 を表すラベルをファイル 1 0 7 に付けていたが、本実施例ではクライアント端末 1 0 1 内のファイル 1 0 7 にはラベルを付けずに、クライアント端末 1 0 1 内に設定する機密レベル制御リスト 1 4 0 0 を用いて情報フロー制御を行い、ファイル 1 0 7 をクライアント端末 1 0 1 外に出す場合にラベルを付け

る。ファイル 1 0 7 をクライアント端末 1 0 1 外に出す場合のラベルのフォーマットは第 1 の実施形態と同様である。

【 0 0 5 8 】

図 1 2 は、本実施例の機密レベル制御リスト 1 4 0 0 を表している。1 列目にファイル名 1 4 0 1、2 列目に当該ファイル 1 0 7 の機密レベル 1 4 0 2、3 列目に当該ファイル 1 0 7 の設定者レベル 1 4 0 3、4 列目に当該ファイル 1 0 7 の設定者 ID 1 4 0 4 が格納されている。

【 0 0 5 9 】

本実施例におけるアプリケーションプログラム 1 0 3 による磁気ディスク 1 0 6 内のファイル 1 0 7 へのアクセスについて説明する。第 1 の実施形態と異なり、本実施例のファイル 1 0 7 にはラベルが付加されていないので、アプリケーションプログラム 1 0 3 が要求するバイトオフセットに処理を施す必要はない。ファイル 1 0 7 の読み取りに関しては、ラベル管理プログラム 1 0 9 はアプリケーションプログラム 1 0 3 が要求するバイトオフセットをそのままファイルシステムドライバ 1 0 4 に渡す。

【 0 0 6 0 】

一方、ファイル 1 0 7 への書き込みに関しては、バイトオフセットの処理を除けば図 6 と同様の処理を行う。つまり、アプリケーションプログラム 1 0 3 によるファイル 1 0 7 への書き込み要求に対して、ラベル管理プログラム 1 0 9 がアプリケーションプログラム 1 0 3 の機密レベル 4 0 2 と当該ファイル 1 0 7 の機密レベル 2 0 2 が一致しているかどうかのチェックを行い、一致していない場合には当該ファイル 1 0 7 の機密レベル 2 0 2 を強制的にアプリケーションプログラム 1 0 3 の機密レベル 4 0 2 に設定し、一致している場合にはファイル 1 0 7 への書き込み要求をファイルシステムドライバ 1 0 4 に送信する。

【 0 0 6 1 】

図 1 3 は、本実施例におけるリムーバブルメディア 1 2 3 のファイル 1 0 7 へのデータ書き込みの処理フロー図である。

ステップ 1 5 0 1 では、アプリケーションプログラム 1 0 3 がリムーバブルメディア 1 2 3 内のファイル 1 2 4 にファイル 1 0 7 のデータを書き込む要求を

出す。

ステップ 1 5 0 2 では、ラベル管理プログラム 1 0 9 はファイル 1 0 7 の機密レベル 2 0 2 をチェックする。

ステップ 1 5 0 3 では、機密レベル 2 0 2 が「社外秘」であるかどうかを確認し、機密レベル 2 0 2 が「一般」の場合にはステップ 1 5 0 4 へ進み、「社外秘」の場合にはステップ 1 5 0 6 へ進む。

【 0 0 6 2 】

機密レベル 2 0 2 が「一般」の場合ステップ 1 5 0 4 では、ラベル管理プログラム 1 0 9 は当該ファイル 1 0 7 のリムーバブルメディア 1 2 3 内のファイル 1 2 4 へ当該ファイル 1 0 7 のデータを書き込む要求を出す。

ステップ 1 5 0 5 では、ファイルシステムドライバ 1 0 4 が書き込み要求を受け取り、ディスクドライバ 1 0 5 がリムーバブルメディア 1 2 3 へ当該 1 0 7 のデータを転送する。

【 0 0 6 3 】

機密レベル 2 0 2 が「社外秘」の場合、ステップ 1 5 0 6 において、ラベル管理プログラム 1 0 9 は当該ファイル 1 0 7 のラベル付きファイルを作成する。

ステップ 1 5 0 7 では、ラベル管理プログラム 1 0 9 は暗号化鍵を生成する。

ステップ 1 5 0 8 では、ラベル管理プログラム 1 0 9 は暗号化鍵を鍵管理サーバ 1 1 4 に登録し、ID番号をサーバから受け取る。

ステップ 1 5 0 9 では、ラベル管理プログラム 1 0 9 は当該ファイル 1 0 7 のラベル付きファイルを、暗号化鍵を用いて暗号化し、暗号化ファイルを作成する。暗号化ファイルはID番号と暗号化データとから成る。ID番号はラベル管理プログラム 1 0 9 が暗号化ファイルの作成時に付加する。

ステップ 1 5 1 0 では、ラベル管理プログラム 1 0 9 は当該ラベル付きファイルをリムーバブルメディア 1 2 3 内のファイル 1 2 4 へ暗号化ファイルのデータを書き込む要求を出し、ステップ 1 5 0 5 へ進む。

【 0 0 6 4 】

本実施例におけるリムーバブルメディア 1 2 3 内にあるファイル 1 2 4 のデータの読み取りは、第 1 の実施例と同様であり、図 8 に従う。また、リムーバブル

メディア 1 2 3 上のファイル 1 2 3 の磁気ディスク 1 0 6 へのコピーまたは移動では、ラベル管理プログラム 1 0 9 は機密レベル制御リスト 1 4 0 0 に当該ファイル 1 2 4 のファイル名 1 4 0 1、機密レベル 1 4 0 2、設定者レベル 1 4 0 3、設定者 ID 1 4 0 4 を追加し、当該ファイル 1 2 4 を磁気ディスク 1 0 6 に保存する。

【 0 0 6 5 】

次に本実施例におけるクライアント端末 1 0 1 でのファイル送信の処理について図 9 を用いて説明する。

ステップ 9 0 1 では、アプリケーションプログラム 1 0 3 がファイル 1 0 7 の送信要求を出す。本実施例においては、ステップ 9 0 2 に進む前に、ラベル管理プログラム 1 0 9 は当該ファイル 1 0 7 の機密レベル 2 0 2 を取得し、ラベル付きファイルを作成する処理ステップを追加している。続く処理は第一の実施例と同様であり、ステップ 9 0 2 へ進み、ラベル管理プログラム 1 0 9 が当該ファイル 1 0 7 の送信要求を、当該ラベル付きファイル 1 0 7 の送信要求に変換する。

ステップ 9 0 3 では、プロトコルドライバ 1 1 0 はパケットに分割し、パケットヘッダを作成する。

ステップ 9 0 4 では、ネットワークアダプタドライバ 1 1 1 は LAN コントローラを経由して外部へファイル 1 0 7 を送信する。

【 0 0 6 6 】

ファイル 1 0 7 の削除要求が発生した場合には、ラベル管理プログラム 1 0 9 は当該ファイル 1 0 7 の削除要求をファイルシステムドライバ 1 0 4 に送信し、ファイルシステムドライバ 1 0 4 から当該ファイル 1 0 7 の削除が成功したというメッセージを受け取ったあとで、ラベル管理プログラム 1 0 9 は機密レベル制御リスト 1 4 0 0 から当該ファイル 1 0 7 の行を削除する。

【 0 0 6 7 】

他のクライアント端末 1 0 1、またはゲートウェイサーバ 1 1 8 からファイル 1 0 7 を受信した場合、ラベル管理プログラム 1 0 9 がファイル 1 0 7 の先頭に付いているラベルをチェックし、機密レベル制御リスト 1 4 0 0 にファイル 1 0 7 のラベル情報の登録を行う。その後、ラベル管理プログラム 1 0 9 はアプリケ

ーションプログラム 1 0 3 に当該ファイル 1 0 7 を渡す。

【 0 0 6 8 】

ファイル 1 0 7 の機密レベル 2 0 2 の変更は、ラベル管理プログラム 1 0 9 が機密レベル変更プログラム 1 0 8 から当該ファイル 1 0 7 の機密レベル 2 0 2 変更要求を受け取り、機密レベル制御リスト 1 4 0 0 を変更することにより行う。具体的には機密レベル制御リスト 1 4 0 0 を用いる点を除き、図 1 0 の処理フローに従う。

【 0 0 6 9 】

第 1 の実施例または第 2 の実施例によれば、ファイル 1 0 7 に機密レベル 2 0 2 を設定し、ネットワークにおける情報フロー制御を行うことが可能となる。

【 0 0 7 0 】

(第 3 の実施例)

次に、ラベルの完全性を保証でき、ラベルの不正な改ざんを防止することが可能な、第 3 の実施形態を説明する。

【 0 0 7 1 】

本実施例によれば、第 3 者がラベルを不正に変更することにより、ラベルを実際に変更したのが誰であるかということ隠すという、更なる不正を防止することが可能になる。つまり、第 3 者 A が不正にラベルを改ざんし、例えば、「社外秘」レベルのファイル 1 0 7 を「一般」に変更し、さらに設定者 ID を他人 B の ID に設定することにより、B が機密レベルを変更したことにする、といった不正を防止することが可能である。すなわち、万一、「社外秘」レベルのファイル 1 0 7 が社外に漏洩しても、覚えのない B が責任を追及される、といったことを防止できる。

【 0 0 7 2 】

図 1 4 は、本実施例で用いるラベル付きファイル 1 0 7 の構造を表す図である。ラベル付きファイル 1 0 7 は、先頭にラベル 1 7 0 1 があり、続いてデータハッシュ値 1 7 0 2、ラベル用署名 1 7 0 3、ファイルデータ 1 7 0 4、リンク用署名 1 7 0 5 からなる。

【 0 0 7 3 】

データハッシュ値1702は、機密レベル202の設定者自身がファイル107を作成、または訂正、または機密レベル202を変更した時点でのファイルデータのハッシュ値である。ラベル用署名1703はラベル1701とデータハッシュ値1702とに対する機密レベル202の設定者によるデジタル署名である。リンク用署名1705はラベル1701とファイルデータ1704とに対するファイルデータ1704の作成者または変更者によるデジタル署名である。

【0074】

ラベル用署名1703によってラベル1701の完全性を保証し、リンク用署名1705によってファイルデータ1704の完全性と、ファイルデータ1704とラベル1701とのリンクの完全性を保証する。ラベル用署名1703とリンク用署名1705を用いることは、万一、情報漏洩が起きた場合に責任の所在を調査する上で有効になるとともに、証拠が残るという意味で不正な情報漏洩を抑止する効果がある。なお、署名生成のための秘密鍵は利用者毎に異なる鍵を持っていることが望ましい。

【0075】

なお、本実施例は第1の実施例の拡張として用いてもよく、その場合にはこのファイル構造をクライアント端末101内外で用いる。また、第2の実施例の拡張として用いる場合には、このファイル構造をクライアント端末101外で用いて、クライアント端末101内では、機密レベル制御リスト1400にデータハッシュ値1702、ラベル用署名1703、リンク用署名1705の列を追加することによりラベル情報の完全性を保証する。

【0076】

以下では、本実施例では第2の実施例を拡張した場合について説明する。

図15は、本実施例でのファイル107へのデータ（ファイルデータ1704）の書き込みの処理フロー図である。

ステップ1801では、アプリケーションプログラム103がファイル107ヘデータ（ファイルデータ1704）の書き込み要求を出す。

ステップ1802では、ラベル管理プログラム109はアプリケーションプログラム103の機密レベル402と当該ファイル107の機密レベル202が一

致しているかをプロセス管理リスト400と機密レベル制御リスト1400を参照してチェックする。

ステップ1803では、アプリケーションプログラム103と当該ファイル107の機密レベル202が一致している場合にはステップ1806へ進み、一致していない場合にはステップ1804へ進む。

【0077】

ステップ1804では、ラベル管理プログラム109は当該ファイル107の機密レベル202をアプリケーションプログラム103の機密レベル402に変更し、さらに、設定者レベル203、設定者ID204についても変更する。

ステップ1805では、ラベル管理プログラム109はデータハッシュ値1702、ラベル用署名1703、リンク用署名1705を、新たに求め、ステップ1808へ進む。ここで、データハッシュ値1702は変更後のファイルデータ1704のハッシュ値であり、ラベル用署名1703とリンク用署名1705はファイル107への書き込み要求者の署名である。

【0078】

ステップ1806では、ラベル管理プログラム109は当該ファイル107の機密レベル202設定者とファイル107への書き込み要求者が一致しているかどうかをチェックし、一致している場合にはステップ1805へ進み、一致していない場合にはステップ1807へ進む。

ステップ1807では、ラベル管理プログラム109はリンク用署名1705を新たに求める。ここでリンク用署名1705はファイル107への書き込み要求者の署名である。

ステップ1808では、ラベル管理プログラム109はファイルシステムドライバ104に対して当該ファイル107へ、上記データハッシュ値1702、ラベル用署名1703、リンク用署名1705のうち新たに求めたものと、ファイルデータ1704の書き込み要求を出す。

ステップ1809では、ファイルシステムドライバは当該ファイルへ書き込むデータをディスクドライバに送信し、ディスクドライバは磁気ディスクに上記データを書き込む。

【 0 0 7 9 】

本実施例におけるクライアント端末 1 0 1 での上記ラベル付きファイル 1 0 7 の送信処理について説明する。まず、ラベル管理プログラム 1 0 9 がアプリケーションプログラム 1 0 3 からファイル送信要求を受け取る。次に、ラベル管理プログラム 1 0 9 はアプリケーションプログラム 1 0 3 からのファイル送信要求を当該ラベル付きファイル 1 0 7 の送信要求に変換する。具体的には、クライアント端末 1 0 1 から送信されるファイル構造は図 1 4 に示す構造と同じである。

【 0 0 8 0 】

図 1 6 は、本実施例でのクライアント端末 1 0 1 におけるファイル受信の処理フロー図である。

ステップ 1 9 0 1 では、ラベル管理プログラム 1 0 9 はラベル付きファイル 1 0 7 を受信する。

ステップ 1 9 0 2 では、ラベル管理プログラム 1 0 9 はラベル付きファイル 1 0 7 のラベル 1 7 0 1 をチェックする。ここでは、ラベル管理プログラム 1 0 9 はラベル用署名 1 7 0 3 からラベル 1 7 0 1 の正当性を検証し、リンク用署名 1 7 0 5 からファイルデータ 1 7 0 4 の完全性と、ファイルデータ 1 7 0 4 とラベル 1 7 0 1 とのリンクの正当性をチェックする。

ステップ 1 9 0 3 では、ステップ 1 9 0 2 でのチェックの結果、ラベル 1 7 0 1、ファイルデータ 1 7 0 4、ファイルデータ 1 7 0 4 とラベル 1 7 0 1 とのリンクが正しい場合にはステップ 1 9 0 4 へ進み、正しくない場合にはステップ 1 9 0 6 へ進む。

【 0 0 8 1 】

ステップ 1 9 0 4 では、ラベル管理プログラム 1 0 9 は当該ラベル付きファイル 1 0 7 のラベル情報を機密レベル制御リスト 1 4 0 0 に追加する。

ステップ 1 9 0 5 では、ラベル管理プログラム 1 0 9 は当該ラベル付きファイル 1 0 7 をアプリケーションプログラム 1 0 3 に渡す。

【 0 0 8 2 】

ステップ 1 9 0 6 では、ラベル管理プログラム 1 0 9 は当該ラベル付きファイル 1 0 7 のラベル情報を管理者に送信する。

ステップ1907では、ラベル管理プログラム109はエラーメッセージをアプリケーションプログラム103に送る。

【0083】

次に、本実施例における「社外秘」であるラベル付きファイル107を「一般」に変更する場合の処理について図10を参考に用いて説明する。。

ステップ1001では、機密レベル変更プログラム108がラベル付きファイル107の機密レベル202を「社外秘」から「一般」に変更する要求を出す。

ステップ1002では、ラベル管理プログラム109は、本実施例においては機密レベル制御リスト1400から当該ラベル付きファイル107の設定者ID204を取得する。

ステップ1003では、ステップ1002で取得した設定者ID204と機密レベル202の変更者IDが一致しているかどうかを判定する。一致している場合には、ステップ1004へ進み、一致していなければステップ1005へ進む。

【0084】

ステップ1004では、ラベル管理プログラム109はラベル付きファイル107の機密レベル202を「一般」に変更し、設定者ID204、設定者レベル203も同時に変更する。本実施例においては、ラベル管理プログラム109は、さらに、ラベル用署名1703、リンク用署名1705を新たに求める処理を行う。

【0085】

ステップ1005以降の処理は第一の実施例と同様であり、ステップ1005において、機密レベル202の変更者が機密レベル202を変更できる権限を持っているかどうかを判定する。権限を持っていればステップ1004へ進み、持っていなければステップ1006へ進む。

ステップ1006では、ラベル管理プログラム109はエラーメッセージを機密レベル変更プログラム108に渡す。

【0086】

上記実施例では、機密レベル202を「社外秘」から「一般」に変更する場合について記述したが、機密レベル202が3レベル以上の場合においても同様の

手法により機密レベル202を下げる事が可能である。

【0087】

図17は、本実施例におけるゲートウェイサーバ118でのラベル1701のチェックの処理フロー図である。

ステップ2101では、組織内のクライアント端末101から外部へ送信するファイル107を受信する。

ステップ2102では、送信管理プログラム119は当該ファイル107のラベル1701の有無をチェックする。

ステップ2103では、ラベル1701が付いていればステップ2104へ進み、付いていなければステップ2111へ進む。

【0088】

ステップ2104では、送信管理プログラム119は当該ラベル付きファイル107の機密レベル202をチェックする。

ステップ2105では、機密レベル202が「一般」であればステップ2106へ進み、「一般」でなければステップ2113へ進む。

【0089】

ステップ2106では、送信管理プログラム119はラベル1701の完全性のチェックを行う。ここでは、送信管理プログラム119はラベル用署名1703からラベル1701の正当性を検証し、リンク用署名1705からファイルデータ1704の完全性と、ファイルデータ1704とラベル1701とのリンクの正当性をチェックする。

ステップ2107では、ステップ2106でのチェックの結果、リンクが正しい場合にはステップ2108へ進み、正しくない場合にはステップ2115へ進む。

【0090】

ステップ2108では、送信管理プログラム119は当該ラベル付きファイル107からラベル1701、データハッシュ値1702、ラベル用署名1703、リンク用署名1705を取り外す。

ステップ2109では、送信管理プログラム119は当該ファイル107を外

部に送信する。

ステップ2110でファイル送信成功となる。

【0091】

ステップ2111では、送信管理プログラム119は当該ファイル107が不正データであると判断し、エラーメッセージを送信元端末に送る。

ステップ2112でファイル送信失敗となる。

【0092】

ステップ2113では、送信管理プログラム119は当該ラベル付きファイル107の機密レベル202が「一般」ではないというメッセージを送信元端末に送る。

ステップ2114でファイル送信失敗となる。

【0093】

ステップ2115では、送信管理プログラム119は当該ラベル付きファイル107のラベルが不正であるというメッセージを送信元端末に送る。

ステップ2116でファイル送信失敗となる。

【0094】

また、送信管理プログラム119は、ファイルの送信元情報と送信先情報と送信ファイル（ラベル1701、データハッシュ値1702、ラベル用署名1703、リンク用署名1705の付いたファイル）の内容全てをログに記憶しておいても良い。

【0095】

本実施例において、ゲートウェイサーバ118が、組織外ネットワーク121からクライアント端末101へ向けて送信されてきたファイル107を受信した場合は、受信管理プログラム120がファイル107に「一般」のラベルを取り付け、クライアント端末101へファイル107を送信する。ここで、ラベルの設定者ID204はゲートウェイサーバ118のIDとし、設定者レベル203は最低レベルに設定する。また、ラベル用署名1703とリンク用署名1705はゲートウェイサーバ118による署名にする。

また、受信管理プログラム120は、ファイル107の送信元情報と送信先情

報と受信ファイルの内容全てをログに記憶しておいても良い。

【 0 0 9 6 】

(第 4 の実施例)

本発明の第 4 の実施形態を説明する。

汎用の計算機上にはさまざまなアプリケーションプログラム 1 0 3 が動作しており、さらに、さまざまなデバイスが接続されており、そのデバイスを操作する為のデバイスドライバが動作している。その為、上記各実施例を汎用の計算機上で実現する場合、アプリケーションプログラム 1 0 3 とデバイスドライバのバグ、さらにはユーザの操作ミスによってラベル情報（機密レベル制御リスト 1 4 0 0）、ラベル管理プログラム 1 0 9、プロセス管理リスト 4 0 0 が変更、削除される脅威がある。本実施例によれば、そのような脅威を防止することが可能である。

図 1 8 は本実施例によるクライアント端末 1 0 1 の構成例であり、図 1 のクライアント端末 1 0 1 に置き換え、上記各実施例に適用することにより、上記効果を得ることができる。

【 0 0 9 7 】

クライアント端末 1 0 1 内には 2 つの OS が動作しており、第 1 の OS が管理するメモリ領域 2 2 0 1 と第 2 の OS が管理するメモリ領域 2 2 0 2 があり、さらにこれら 2 つの OS を制御する複数 OS 制御プログラム 2 2 0 4 が動作している。複数 OS 制御技術に関しては、たとえば、特開平 1 1 - 1 4 9 3 8 5 号公報に開示されている。

【 0 0 9 8 】

また、第 1 の OS が管理するメモリ領域 2 2 0 1 内には、アプリケーションプログラム 1 0 3、機密レベル変更プログラム 1 0 8、I/O フックプログラム 2 2 0 3、ファイルシステムドライバ 1 0 4、ディスクドライバ 1 0 5、プロトコルドライバ 1 1 0、ネットワークアダプタドライバ 1 1 1 がロードされており、また、第 1 の OS は磁気ディスク 1 0 6、ネットワーク I/F 1 1 2 を管理しており、磁気ディスク 1 0 6 内にはファイル 1 0 7 が格納されている。

【 0 0 9 9 】

第2のOSが管理するメモリ領域2202内には、ラベル管理プログラム109、プロセス管理リスト400があり、また、第2のOSは磁気ディスク2205を管理しており、磁気ディスク2205内には機密レベル制御リスト1400が格納されている。

【0100】

I/Oフックプログラム2203はアプリケーションプログラム103または機密レベル変更プログラム108からのファイル107へのアクセス要求またはファイル107の送受信要求をフックする。さらに、I/Oフックプログラム2203はラベル管理プログラム109に処理を依頼する機能とラベル管理プログラム109の処理結果を受け取りファイルシステムドライバ104またはプロトコルドライバ110に処理結果を渡す機能を持っている。具体的にはI/Oフックプログラム2203は複数OS制御プログラム2204のOS間通信機能を利用してラベル管理プログラム109に処理を依頼する。OS間通信機能に関しては、たとえば、特開平11-85546号公報に開示されている。

【0101】

本実施例によれば、保護対象（ラベル管理プログラム109、プロセス管理リスト400、機密レベル制御リスト1400）を第2のOSが管理することにより、第1のOS上で動作しているアプリケーションプログラム103、デバイスドライバのバグまたはユーザの操作ミスによる変更から保護することが可能となる。

【0102】

（その他）

上記各実施例によれば、単に組織内の機密情報の漏洩を防止だけでなく、組織外ネットワーク121経由での不正侵入による機密情報の漏洩も防止することも可能になる。不正侵入者がゲートウェイサーバ118を経由してクライアント端末101内の機密ファイルを持ち出そうとした場合、ゲートウェイサーバ118の送信管理プログラム119は、当該機密ファイルのラベルをチェックする。機密レベルが「社外秘」の場合、送信管理プログラム119は外部への送信を拒否する為、機密ファイルの漏洩を防止することが可能である。

【0103】

また、信頼できない (Untrusted) プログラム (例：メールに添付されてくるプログラム) に対しては、ラベル管理プログラム 1 0 9 が「Untrusted」というラベルを取り付け、アクセスできるファイルに制限を加えるように構成することも可能である。

具体的にはシステムファイルやカーネルの設定情報ファイルに「Trusted」のラベルを付け、「Untrusted」のプログラムが「Trusted」のファイルへアクセスした場合に、ラベル管理プログラム 1 0 9 がアクセス制限を加えるように構成すればよい。この機能は、たとえば、ファイルオープン時にラベル管理プログラム 1 0 9 がプログラムとファイルのラベルをそれぞれチェックすることにより実現可能になる。このような機能を用いれば、コンピュータウイルスによるシステムへの影響を最小限に抑えることが可能である。

【 0 1 0 4 】

また、専用の通信プロトコルを用いて、クライアント端末 1 0 1 とゲートウェイサーバ 1 1 8 間の通信を行ってもよい。これにより、例えば、各パケットのヘッダ領域にラベルを付加し、ゲートウェイサーバ 1 1 8 の送信管理プログラム 1 1 9 はこのパケットのヘッダ領域のラベルをチェックすることによりデータの送信の可否を決定することが可能となる。専用の通信プロトコルを用いた場合は、データを組織外ネットワーク 1 2 1 へ送信する場合には、送信管理プログラム 1 1 9 はラベルを取り除き、汎用の通信プロトコル (TCP/IP など) のパケットに変換するように構成すればよい。

【 0 1 0 5 】

また、電子メールの添付ファイルにラベル付きのファイル 1 0 7 を添付して送信し、ゲートウェイサーバ 1 2 1 では、メールの添付ファイルのラベルをチェックすることにより、電子メールによって機密ファイルが社外に漏洩することを防止することが可能である。なお、メール本文に関しては、キーワード検索によってポリシーに反するキーワードが含まれていないかどうかをチェックすることにより、漏洩防止が可能になる。

【 0 1 0 6 】

また、クライアント端末 1 0 1 毎に機密レベルを設定し、さらにクライアント

端末 1 0 1 間と、クライアント端末 1 0 1 と各サーバ間に中間サーバを設け、中間サーバに情報漏洩防止機能を持たせても良い。この場合、クライアント端末 1 0 1 上のファイル 1 0 7 にはラベルを付けなくてもよい。

【0 1 0 7】

この例において、中間サーバは各クライアント端末 1 0 1 の機密レベルを管理し、クライアント端末 1 0 1 が送信したファイル 1 0 7 を別のクライアント端末 1 0 1 あるいは他の部署あるいはグループに送信してよいかどうかを決定する。中間サーバはクライアント端末 1 0 1 に直接ファイル 1 0 7 を送信する場合にはラベルを取りつけず、他の部署あるいはグループの中間サーバに送信する場合にはラベルを取りつける。中間サーバは別の中間サーバから受信したファイル 1 0 7 のラベルをチェックし、クライアント端末 1 0 1 に送信する場合にはラベルを取り外してファイル 1 0 7 を送信する。なお、中間サーバは部署単位あるいはグループ単位に設けても良い。

【0 1 0 8】

このようにすることにより、各クライアント端末 1 0 7 にはラベル管理プログラム 1 0 9 を組み込む必要がなくなり、情報漏洩防止機能を導入する為の手間を軽減できる。

【0 1 0 9】

【発明の効果】

機密ファイルの漏洩を防止することが、任意のファイルフォーマットに対して対応可能なシステムを提供できる。

【0 1 1 0】

【符号の説明】

1 0 1 : クライアント端末、1 0 2 : メモリ、1 0 3 : アプリケーションプログラム、1 0 4 : ファイルシステムドライバ、1 0 5 : ディスクドライバ、1 0 6 : 磁気ディスク、1 0 7 : ファイル、1 0 8 : 機密レベル変更プログラム、1 0 9 : ラベル管理プログラム、1 1 0 : プロトコルドライバ、1 1 1 : ネットワークアダプタドライバ、1 1 2 : ネットワーク I/F、1 1 3 : CPU、1 1 4 : 鍵管理サーバ、1 1 5 : 鍵管理プログラム、1 1 6 : 鍵情報、1 1 7 : 組織内ネッ

トワーク、118:ゲートウェイサーバ、119:送信管理プログラム、120:受信管理プログラム、121:組織外ネットワーク、122:外部記憶装置、123:リムーバブルメディア、124:ファイル、201:バージョン情報、202:機密レベル、203:設定者レベル、204:設定者ID、400:プロセス管理リスト、401:プロセスID、402:プロセス機密レベル、403:ファイル名、404:ファイルの機密レベル、1400:機密レベル制御リスト、1401:ファイル名、1402:機密レベル、1403:設定者レベル、1404:設定者ID、1701:ラベル、1702:データハッシュ値、1703:ラベル用署名、1704:ファイルデータ、1705:リンク用署名、2201:第1のOSが管理するメモリ領域、2202:第2のOSが管理するメモリ領域、2203:I/Oフックプログラム、2204:複数OS制御プログラム、2205:磁気ディスク。

【0111】

【図面の簡単な説明】

【図1】

本発明によるネットワークシステムの全体を表す図である。

【図2】

ラベルのフォーマットを表す図である。

【図3】

ファイルオープンの処理フロー図である。

【図4】

プロセス管理リストを表す図である。

【図5】

ファイルの読み取りの処理フロー図である。

【図6】

ファイルへの書き込みの処理フロー図である。

【図7】

リムーバブルメディアへのファイルの書き込みの処理フロー図である。

【図8】

リムーバブルメディアからのファイルの読み取りの処理フロー図である。

【図 9】

ファイルのネットワーク上への送信の処理フロー図である。

【図 1 0】

機密レベルの変更の処理フロー図である。

【図 1 1】

ゲートウェイサーバでのラベルのチェックの処理フロー図である。

【図 1 2】

機密レベル制御リストのフォーマットを表す図である。

【図 1 3】

第 2 の実施例におけるリムーバブルメディアへのファイルの書き込みの処理フロー図である。

【図 1 4】

第 3 の実施例におけるラベル付きファイルの構造を表す図である。

【図 1 5】

第 3 の実施例におけるファイルへの書き込みの処理フロー図である。

【図 1 6】

クライアント端末におけるファイル受信の処理フロー図である。

【図 1 7】

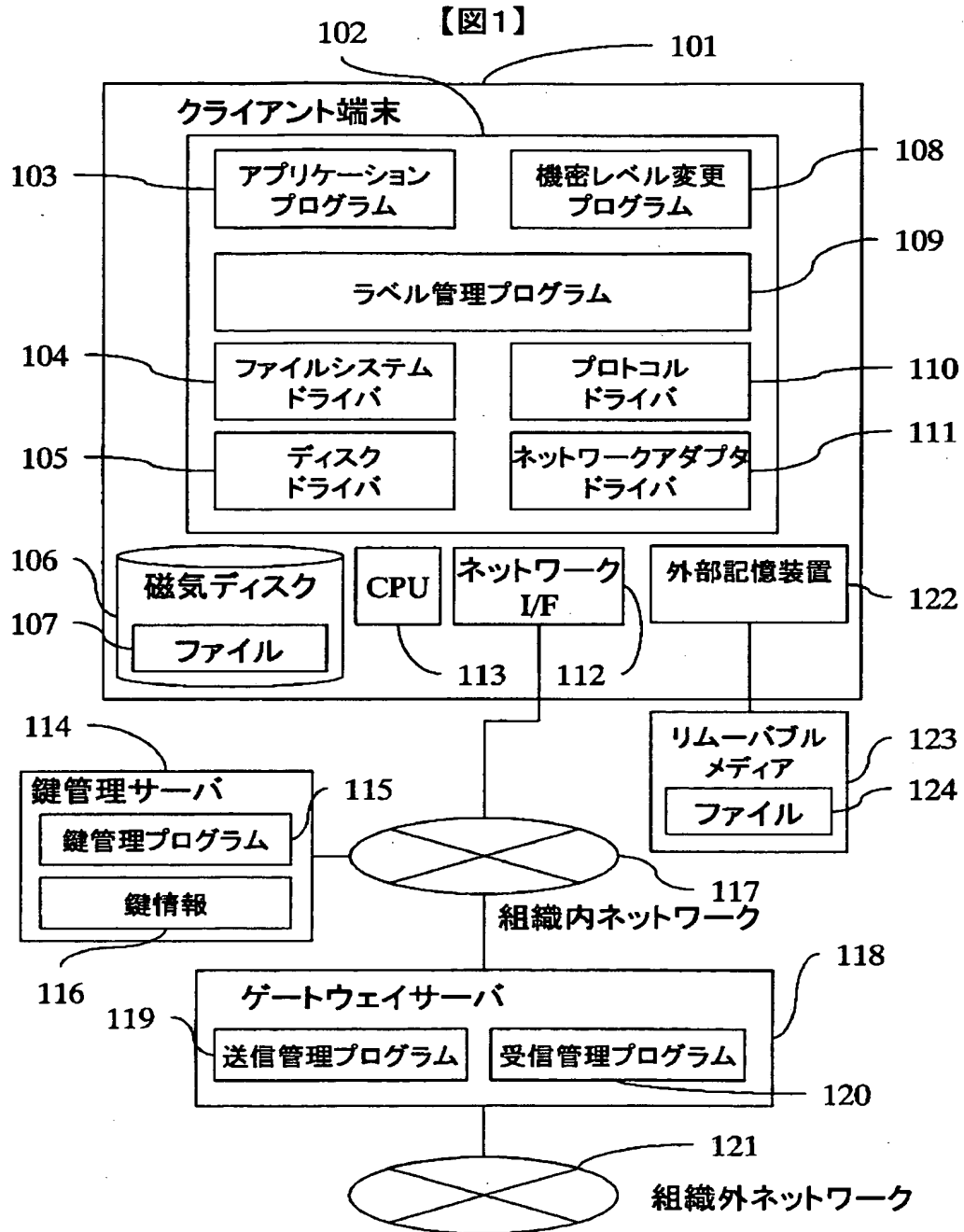
第 3 の実施例におけるゲートウェイサーバでのラベルのチェックの処理フロー図である。

【図 1 8】

2 つの OS を利用した本発明によるネットワークシステムのクライアント端末の構成図である。

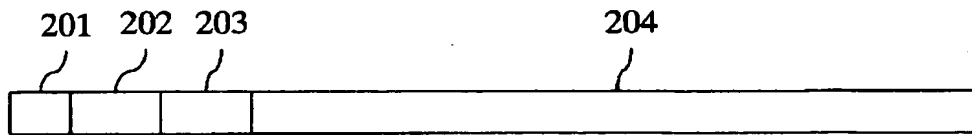
【書類名】 図面

【図1】



【図 2】

【図 2】



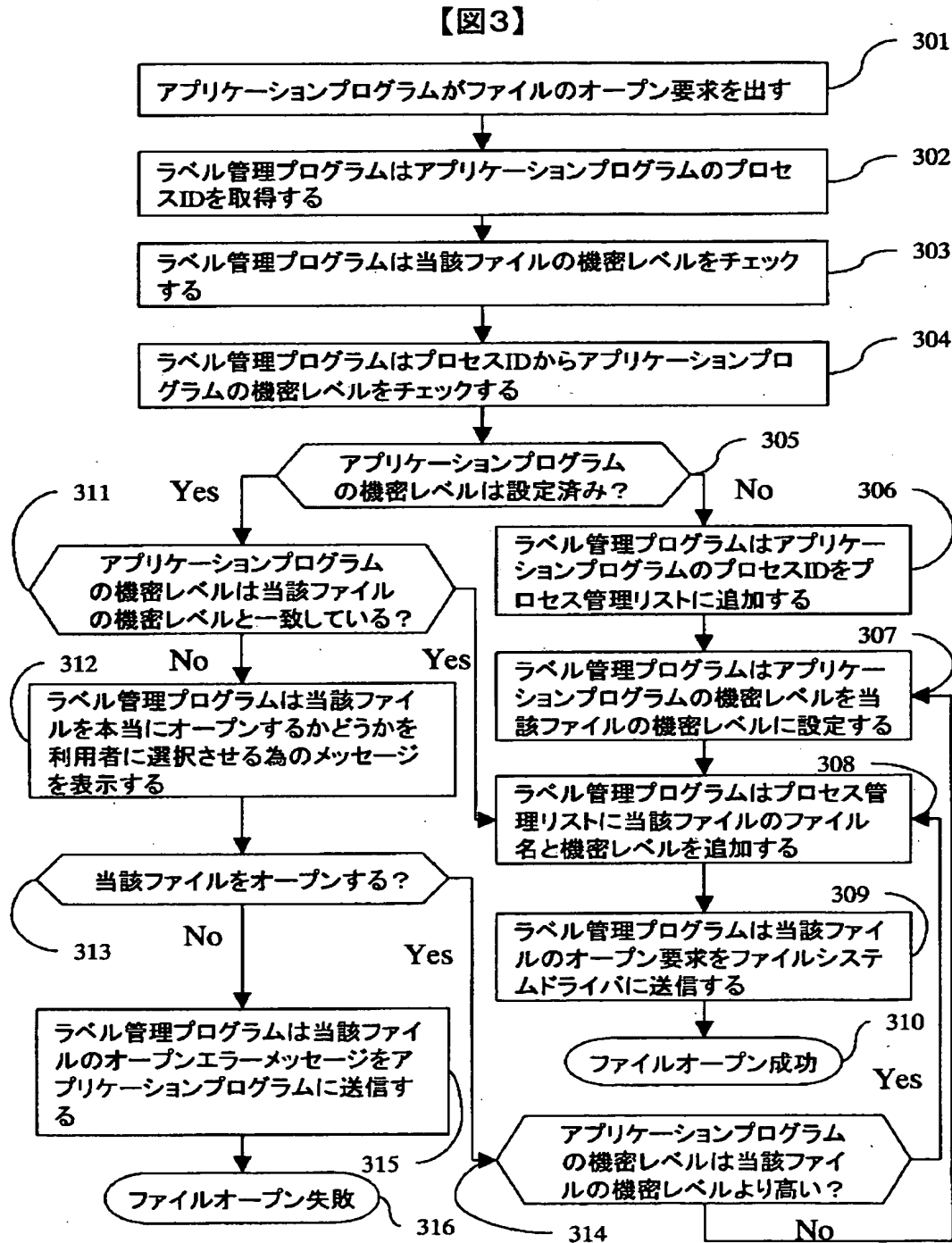
201: バージョン情報 (2bit)

202: 機密レベル (3bit)

203: 設定者レベル (3bit)

204: 設定者ID (24bit)

【図3】



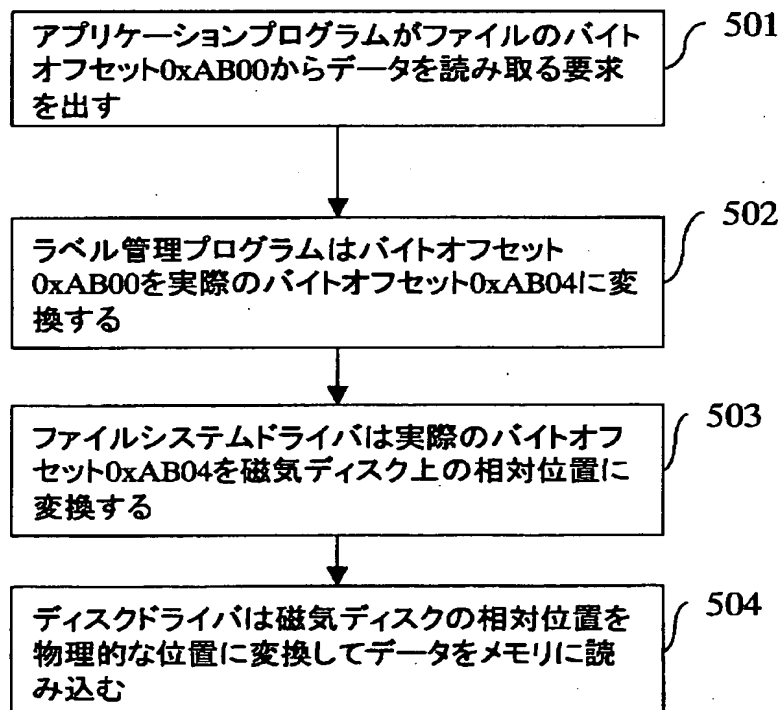
【図 4】

【図 4】

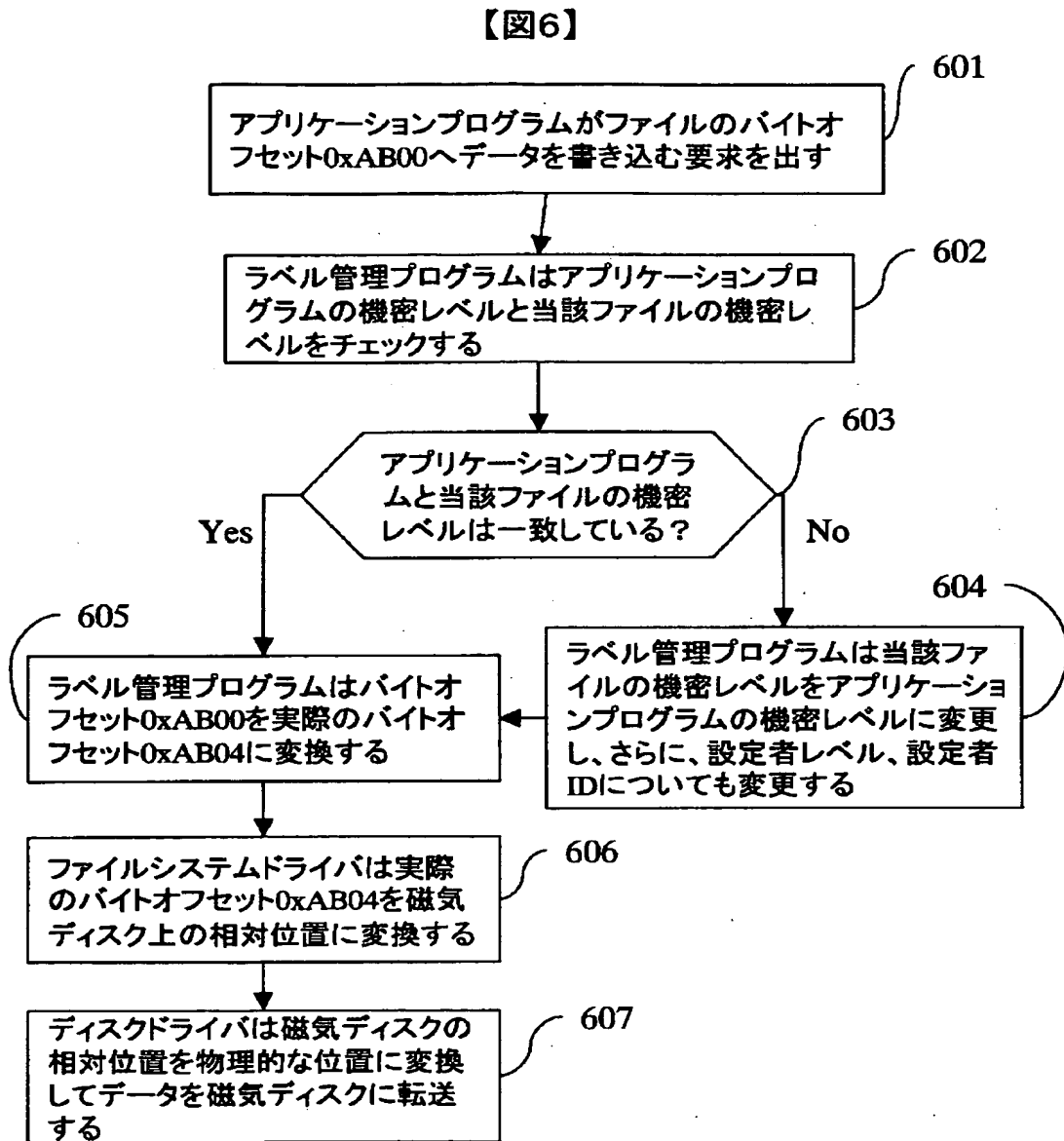
プロセスID	プロセス機密レベル	ファイル名	ファイルの機密レベル
FF053EC9	社外秘	C:\document\file1.dat	社外秘
		C:\document\file2.dat	一般
FF039D33	一般	C:\document\file3.dat	一般
...

【図 5】

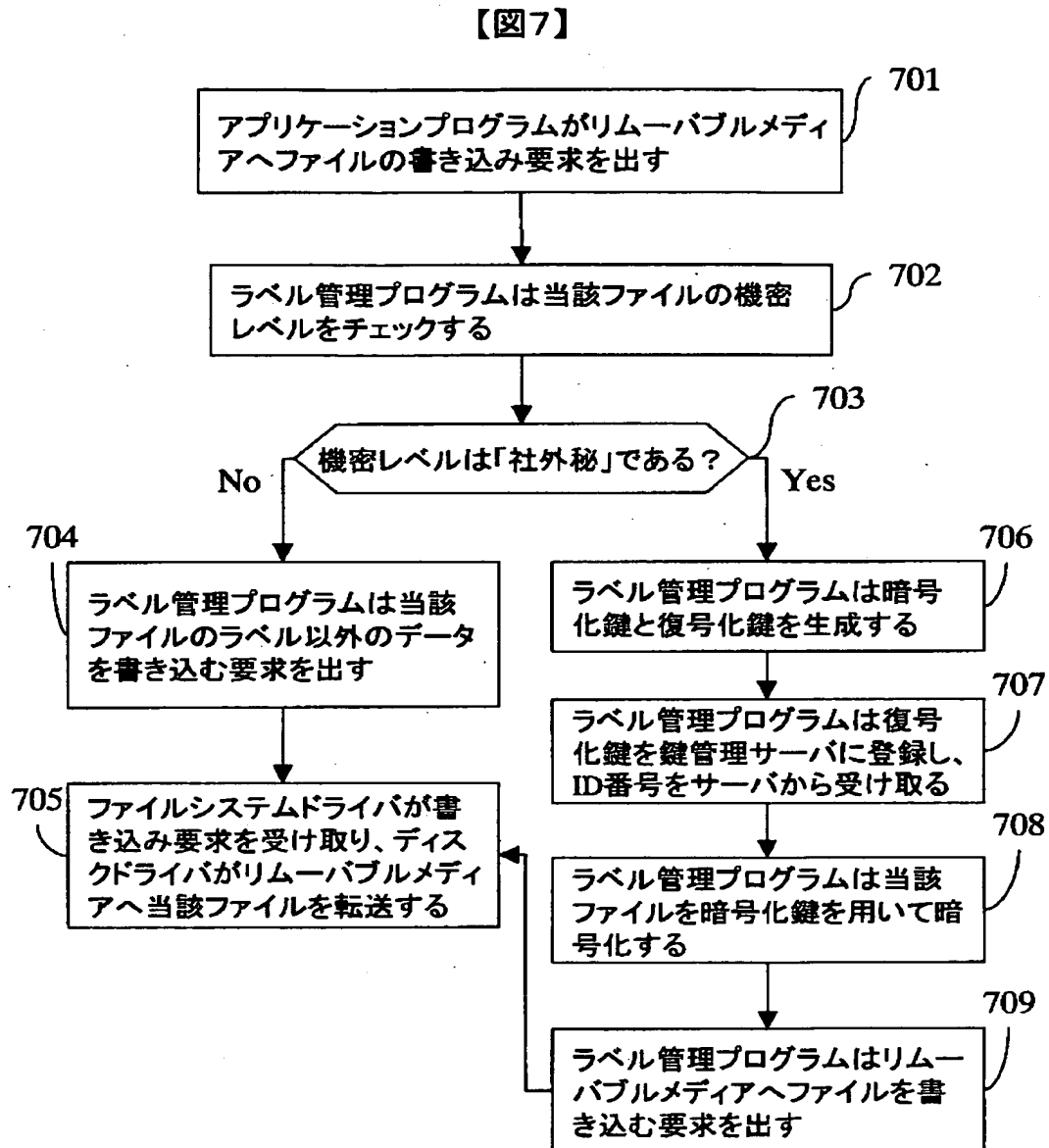
【図 5】



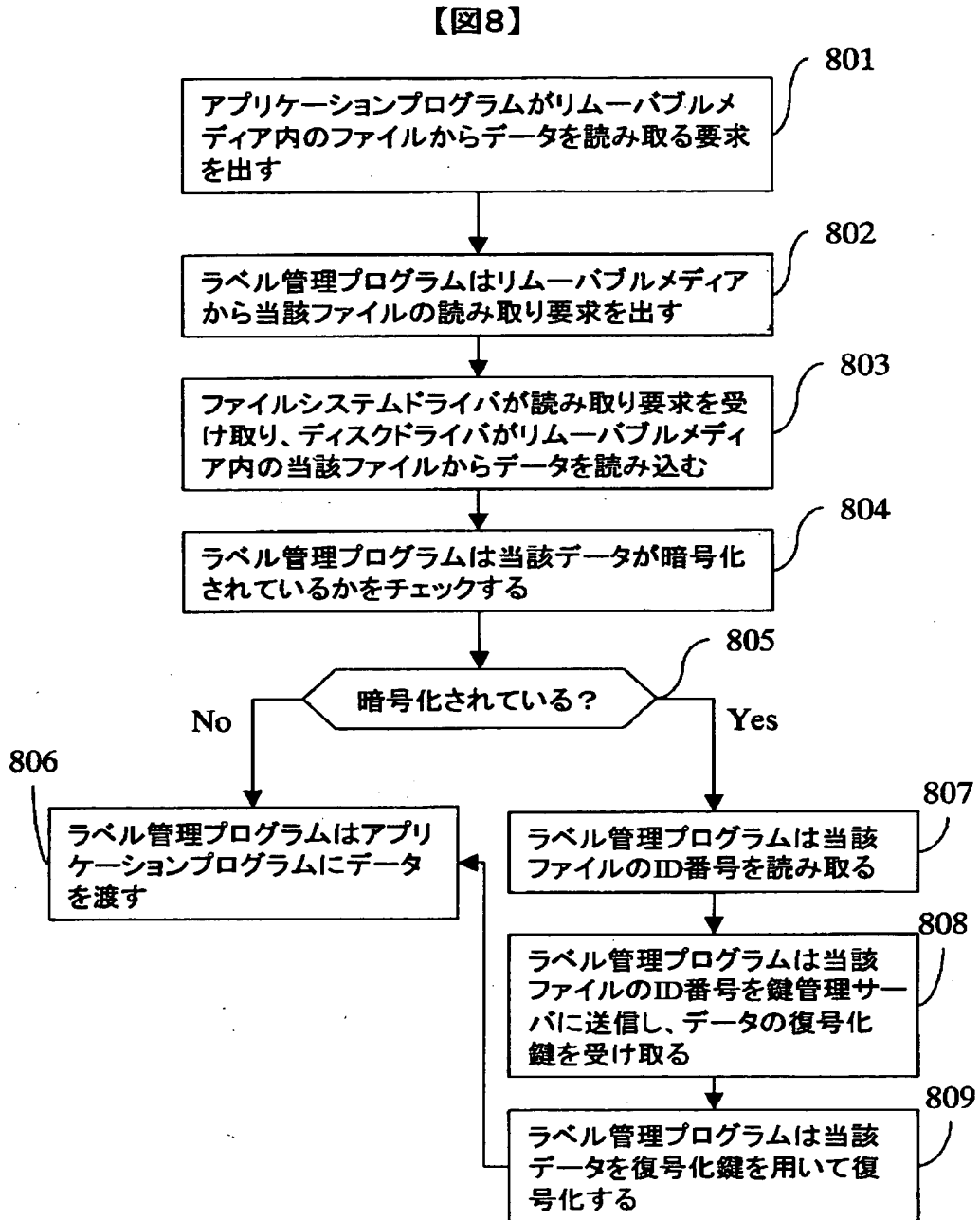
【図 6】



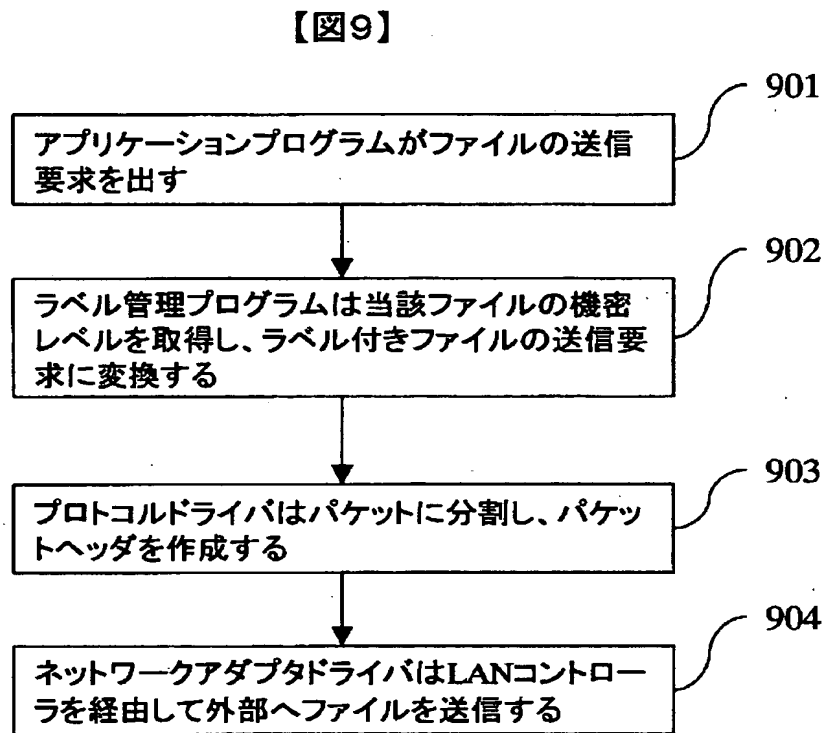
【図 7】



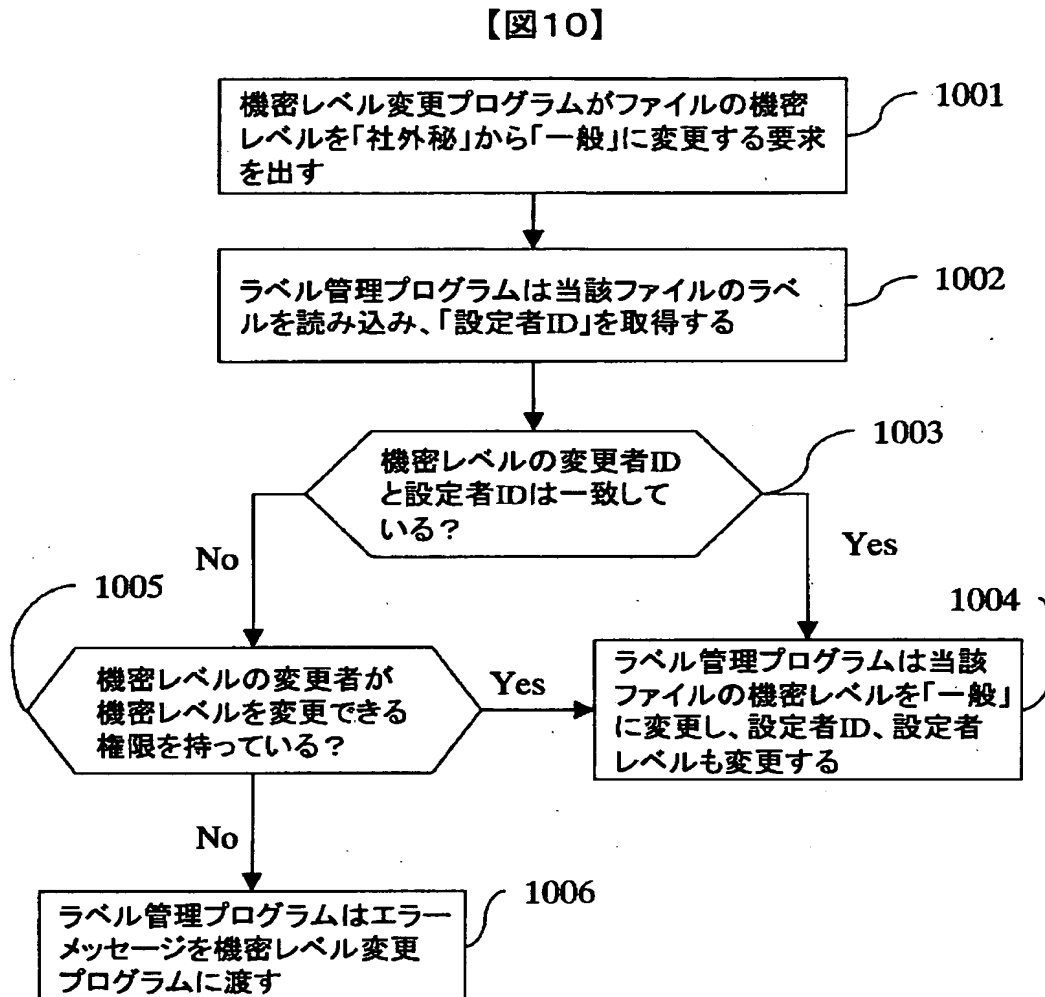
【図 8】



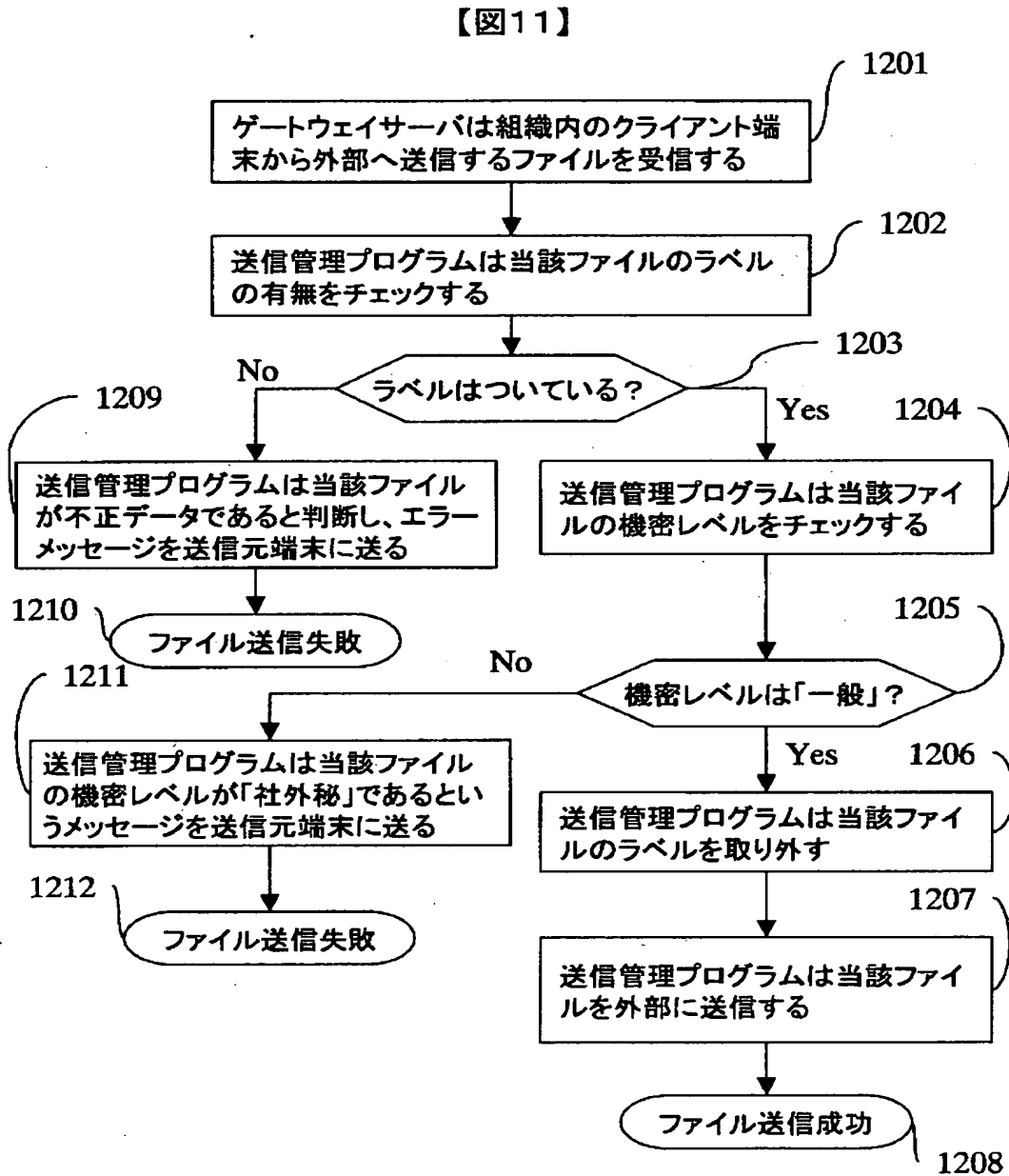
【図 9】



【図10】



【図 11】



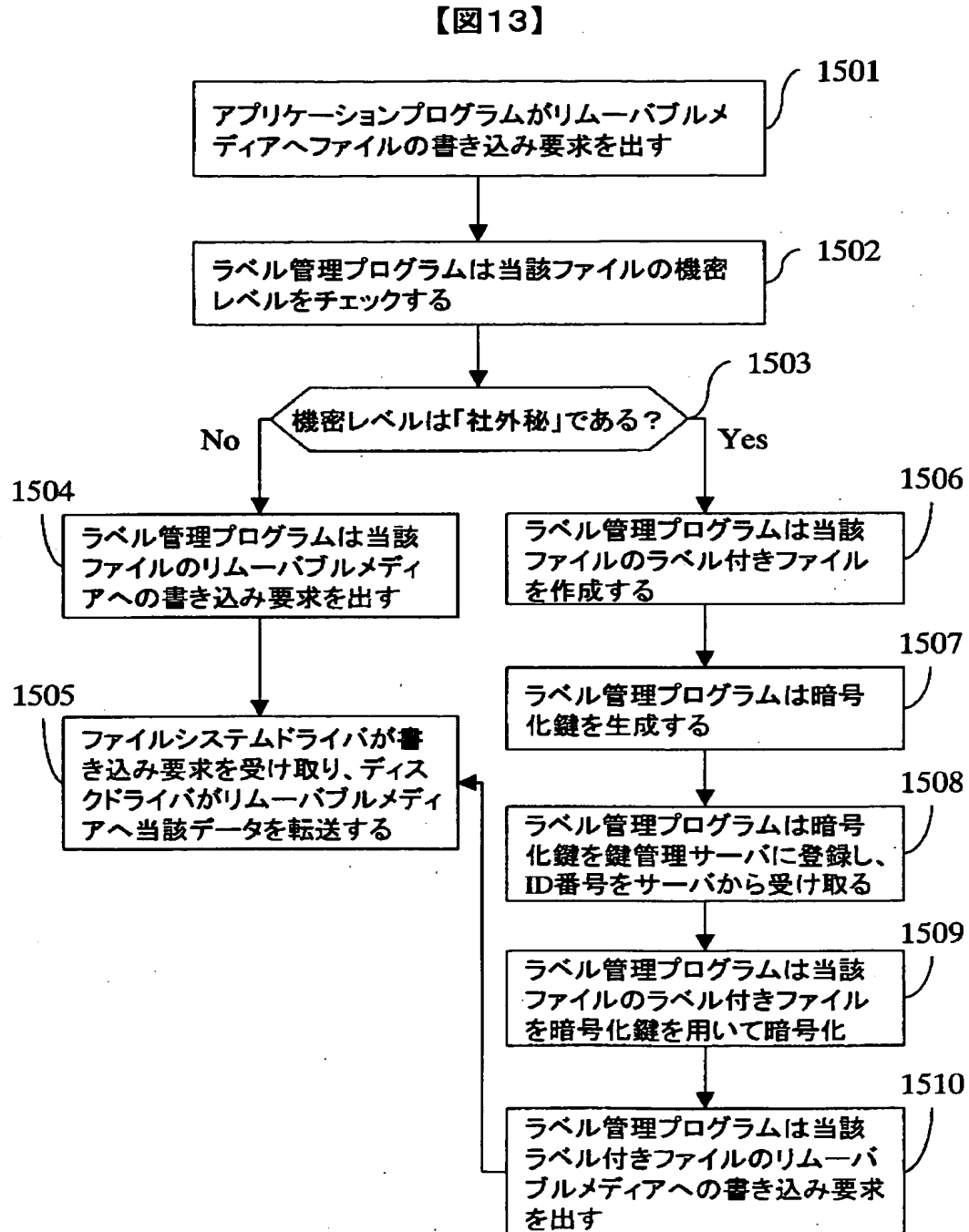
【図 1 2】

【図12】

1400

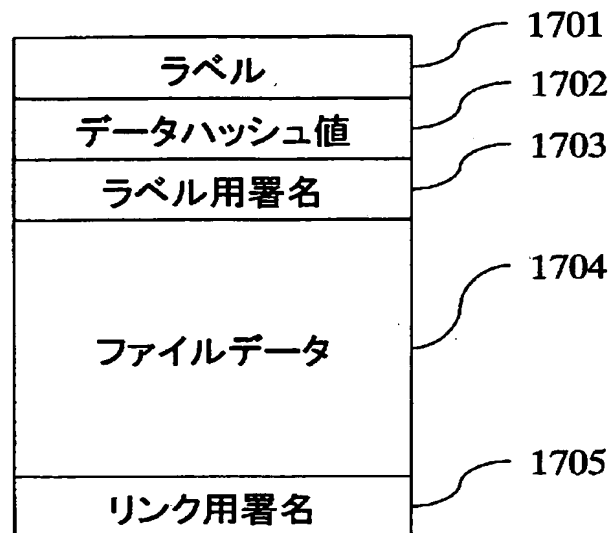
1401	1402	1403	1404
ファイル名	機密レベル	設定者レベル	設定者ID
C:\document\file1.dat	社外秘	一般	12345678
C:\document\file2.dat	一般	一般	12345678
...

【図13】

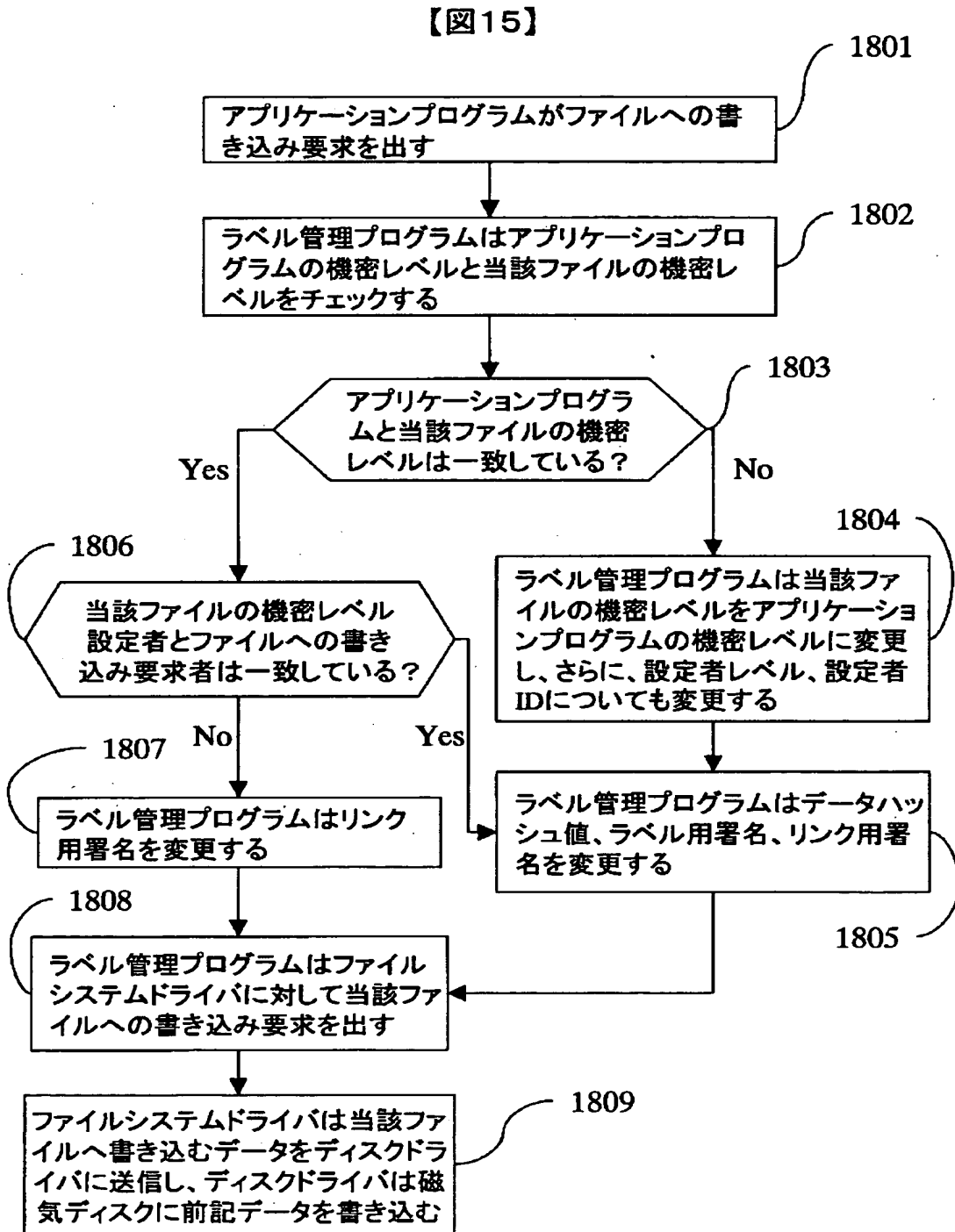


【図 1 4】

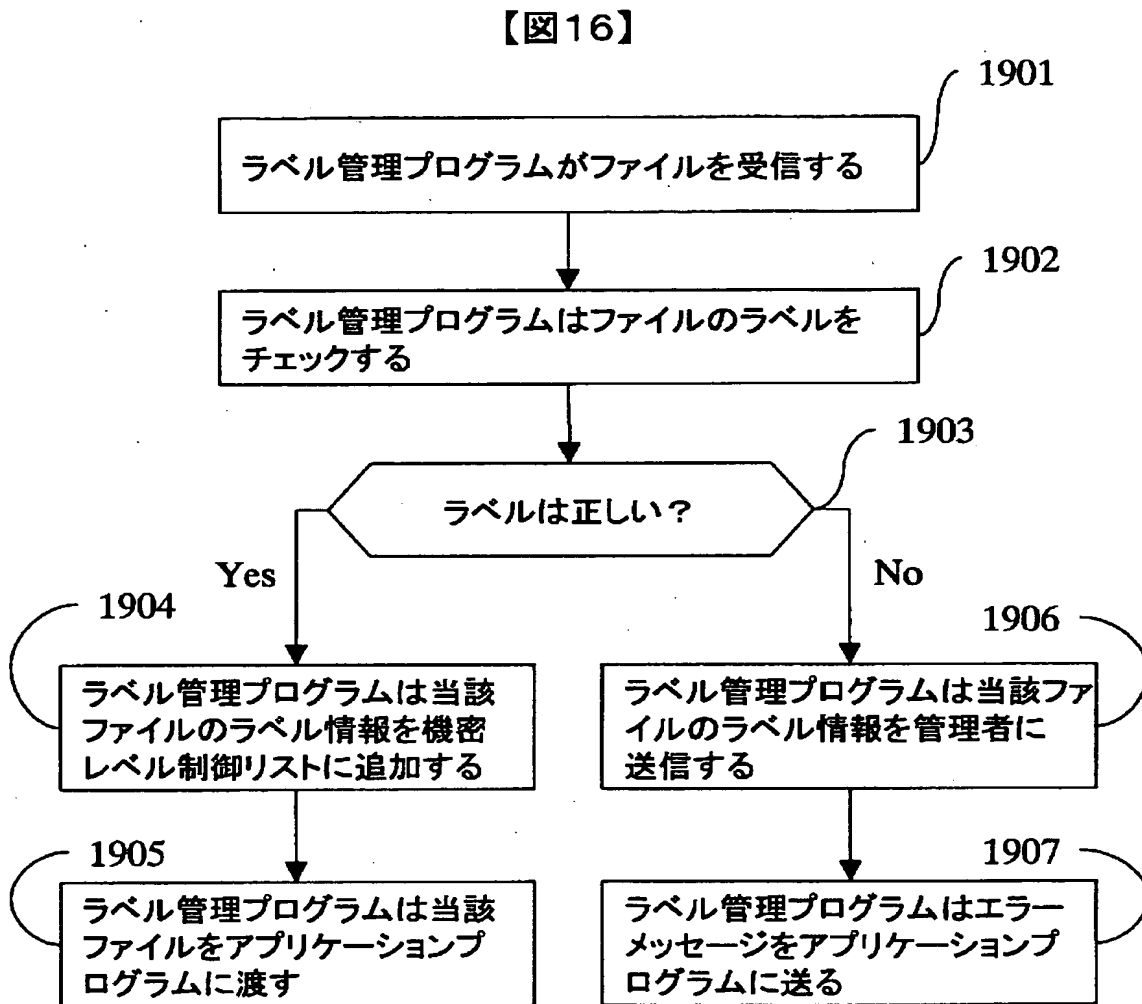
【図14】



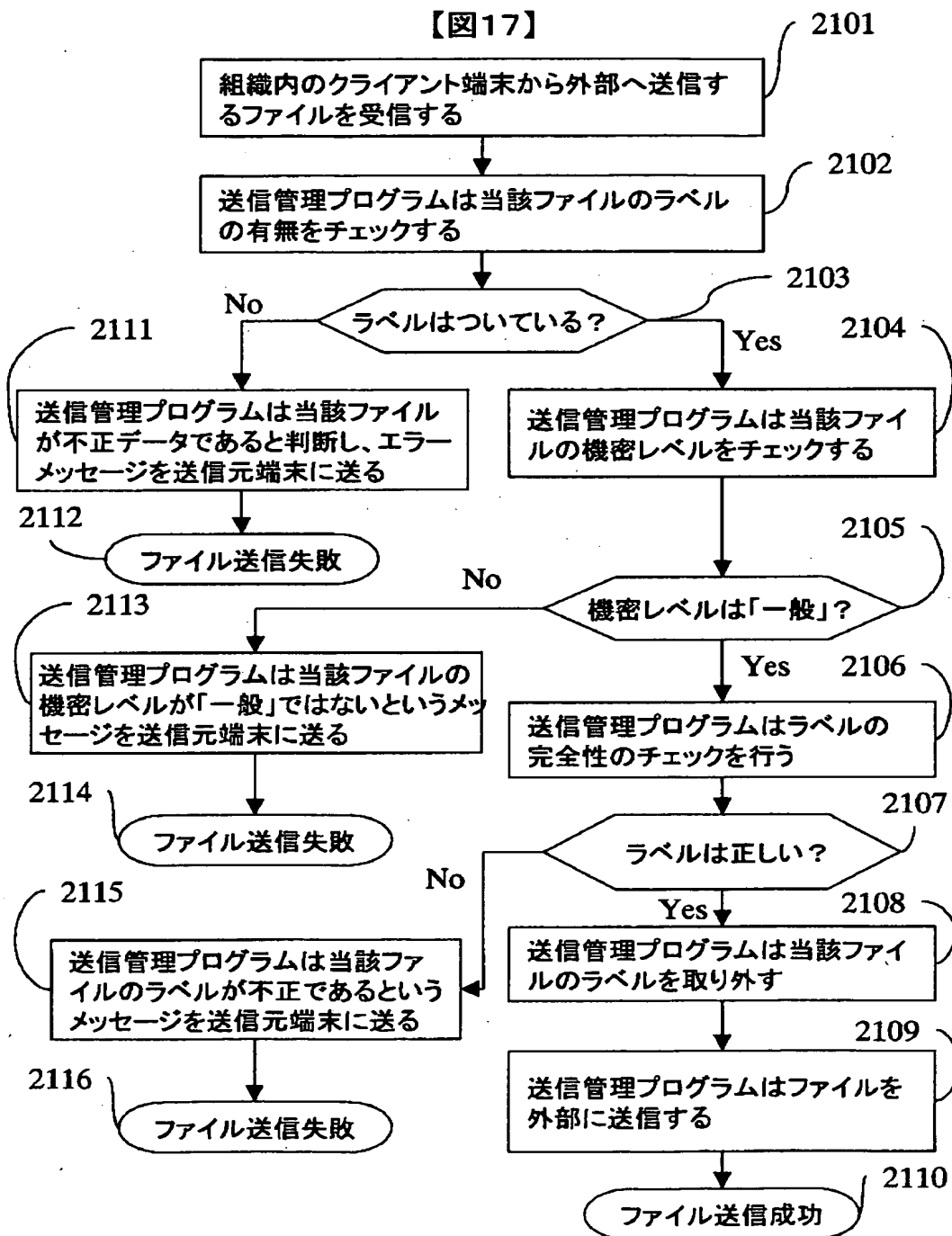
【図 1 5】



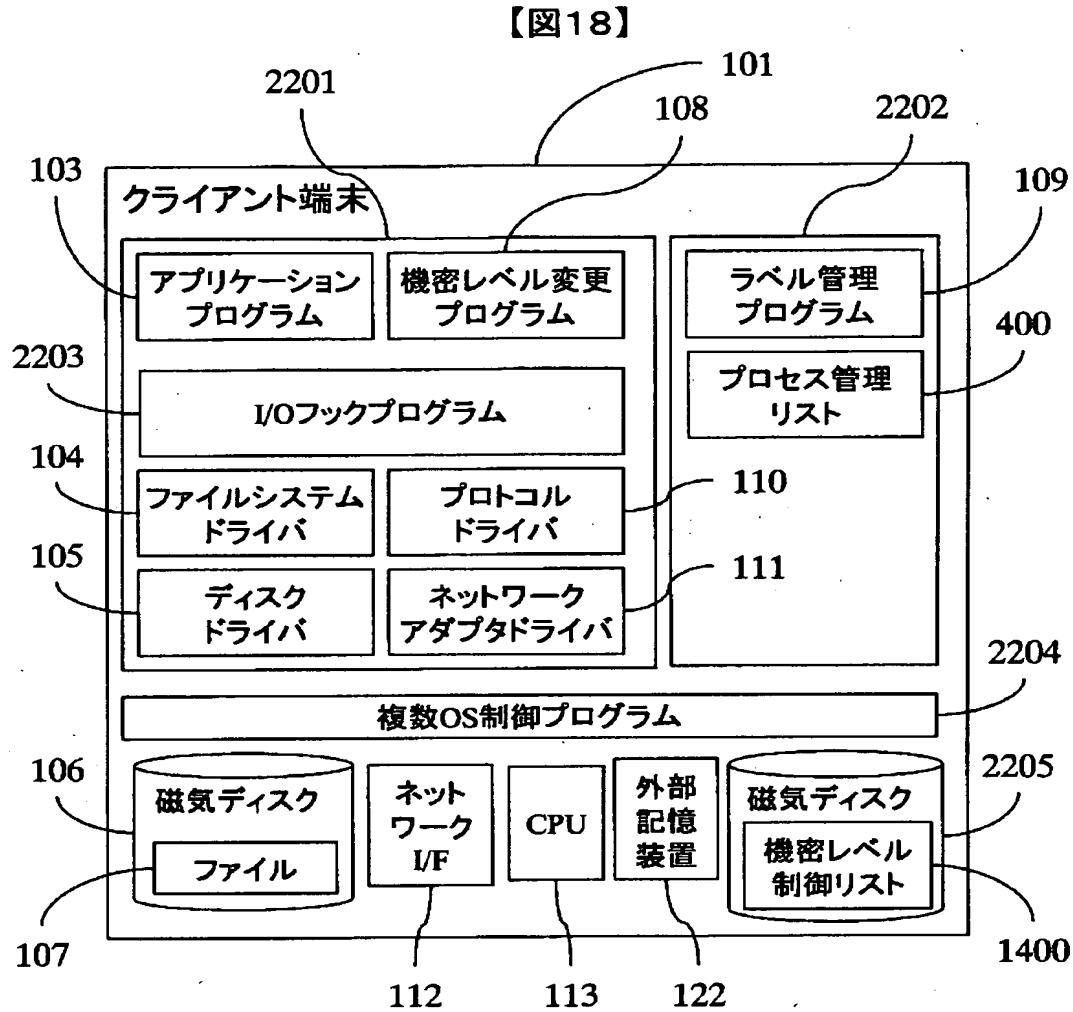
【図 1 6】



【図 17】



【図18】



【書類名】 要約書

【要約】

【課題】

送信者の不注意による機密ファイルの漏洩を防止すると同時に、任意のファイルフォーマットに対して対応可能なネットワークシステムを提供する。

【解決手段】

クライアント端末 1 0 1 内のファイル 1 0 7 に機密レベル（機密、非機密）を表すラベルを付け、クライアント端末 1 0 1 はラベル付きファイル 1 0 7 を外部へ送信する。ゲートウェイサーバ 1 1 8 上の送信管理プログラム 1 1 9 がファイル 1 0 7 のラベルのチェックを行い、機密レベルが非機密の場合に組織外ネットワーク 1 2 1 へファイル 1 0 7 を送信する。また、ラベル管理プログラム 1 0 9 がクライアント端末 1 0 1 内のラベル付きファイル 1 0 7 の管理を行う。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2001-370824
受付番号	50101782664
書類名	特許願
担当官	第八担当上席 0097
作成日	平成13年12月 6日

<認定情報・付加情報>

【提出日】	平成13年12月 5日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所